ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Методи підвищення ефективності систем IoT»

на здобуття освітнього ступеня бакалавр

зі спеціальності 126 Інформаційні системи та технології
(код,найменування спеціальності)

освітньо-професійної програми Інформаційні системи та технології
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олександр ГУДИМ
(підпис) *(ім'я, ПРІЗВИЩЕ здобувача)*

Виконав:

здобувач вищої освіти

групи ІСД-41 Олександр ГУДИМ
(ім'я,ПРІЗВИЩЕ)

Керівник: Олег СЕНЬКОВ

канд. техн. наук. *(ім'я,ПРІЗВИЩЕ)*

Рецензент:

_____

науковий ступінь *(ім'я,ПРІЗВИЩЕ)*

вчене звання

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Інформаційних систем та технологій

Ступінь вищої освіти бакалавр

Спеціальність 126 Інформаційні системи та технології

Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІСТ
_____ Каміла СТОРЧАК
“____” _____2026 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Гудим Олександр Олександрович

(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Методи підвищення ефективності систем IoT»

керівник кваліфікаційної роботи: Олег СЕНЬКОВ, канд. техн. наук.
(ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20” лютого 2026 р. №51

2. Строк подання кваліфікаційної роботи «01» червня 2026 р.

3. Вихідні дані кваліфікаційної роботи:

- Наукові та навчально-методичні джерела з питань архітектури, протоколів і технологій Інтернету речей.
- Відомості про сучасні мережеві технології, хмарні сервіси та засоби забезпечення безпеки IoT-систем.
- Практичні приклади застосування Інтернету речей у промисловості, транспорті, медицині та концепції розумних міст.
-

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

1. Інтернет речей
2. Мережева архітектура IoT-систем;
3. Застосування хмарних технологій в IoT та перспективи їх розвитку.
4. Застосування технологій кіберзахисту в IoT
5. Аналіз ефективності мережних технологій в IoT

5.Перелік ілюстраційного матеріалу: *презентація*

6. Дата видачі завдання « 20» лютого 2026р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	11.11.2025	Виконано
2	Огляд літератури	11.12.2025	Виконано
3	Вступ	29.12.2025	Виконано
4	Дослідження перспектив розвитку мережевих технологій в Інтернеті речей	23.03.2026	Виконано
5	Огляд хмарних технологій та Інтернету речей	6.04.2026	Виконано
6	Огляд прикладів застосування технологів кібербезпеки в Інтернеті речей	26.04.2026	Виконано
7	Аналіз прикладів взаємодії мережевих ресурсів та хмарних технологів в Інтернеті речей	11.05.2026	Виконано
8	Оформлення дипломної роботи	18.05.2026	Виконано

Здобувач вищої освіти _____ Олександр ГУДИМ

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник

кваліфікаційної роботи _____ Олег СЕНЬКОВ

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 86 стор., 4 табл., 23 рис., 65 джерел.

В роботі комплексно розглянуто питання стосовно мережевих технологій Інтернету речей, а саме архітектуру, принцип їх інтеграції, переваги, виклики та недоліки. Також було досліджено перспективи мережевих технологій в Інтернеті речей. Особлива увага була приділена аналізу прикладів застосування мережевих технологій в Інтернеті речей, зокрема, в розумних містах.

Метою роботи є дослідження та аналіз інтеграції технології Інтернету речей (IoT) з мережевими, зокрема, безпроводовими технологіями, у сполученні із хмарними та безпековими технологіями, аналіз переваг та викликів їх інтеграції та перспективи подальшого розвитку для визначення ключових методів підвищення ефективності мереж Інтернету речей.

Об'єкт дослідження - процес функціонування та взаємодії пристроїв, мереж і програмних компонентів у системах Інтернету речей (IoT).

Предмет дослідження - Архітектура, принципи функціонування та основні технології побудови систем Інтернету речей.

Короткий зміст роботи: У роботі розглянуто концепцію Інтернету речей та передумови її розвитку. Проаналізовано основні компоненти IoT-систем, зокрема сенсори, виконавчі механізми, мережеві технології та хмарні обчислення. Досліджено архітектурні моделі Інтернету речей і особливості їх побудови. Розглянуто сфери застосування IoT у промисловості, транспорті, медицині, розумних будинках і містах. Також проаналізовано питання інформаційної безпеки та перспективи розвитку технологій Інтернету речей.

КЛЮЧОВІ СЛОВА: Інтернет речей, протоколи IoT, архітектура мережі IoT, тенденції розвитку, хмарні технології, взаємодія хмари та IoT, віртуалізація, автоматизація, SAAS, PAAS, IAAS, безпека IoT, машинне навчання, обробка даних, масштабованість, ефективність.

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

«e-government»	Модель державного управління, яка заснована на використанні сучасних інформаційних та комунікаційних технологій
3G	Третє покоління технології мобільного зв'язку
4G	Четверте покоління технології мобільного зв'язку
5G	П’яте покоління технології мобільного зв'язку
AES	Симетричний алгоритм блочного шифрування (Advanced Encryption Standard)
API	Інтерфейс програмування застосунків (Application Programming Interface)
ARPANET	Мережа передових досліджень (Advanced Research Projects Agency Network)
AWS	Amazon Web Services
CoAP	Спеціалізований протокол інтернет-додатків на основі UDP для пристроїв з обмеженими можливостями (Constrained Application Protocol)
CPU	Центральний процесор (Central Processing Unit)
DDoS	Атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні (Distributed Denial-of-Service)
GDPR	Загальний регламент про захист даних (General Data Protection Regulation)
GPS	Система глобального позиціювання (Global Positioning System)
HR	Людські ресурси (Human resources)
http	Протокол передачі даних, що використовується в комп'ютерних мережах (Hypertext Transfer Protocol)

https	Розширення протоколу передачі гіпертексту (HTTP), що використовує шифрування для безпечного спілкування через комп'ютерну мережу
IaaS	Інфраструктура як послуга (Infrastructure as a Service)
IEEE	Інститут інженерів з електротехніки та електроніки (Institute of Electrical and Electronics Engineers)
IIoT	Промисловий Інтернет речей (Industrial Internet Of Things)
IoT	Інтернет речей (Internet of Things)
IT	Інформаційні технології (Information Technology)
ITU	Міжнародний союз електрозв'язку (International Telecommunication Union)
LAN	Локальна мережа (Local area network)
LoRaWAN	Бездротовий мережевий протокол, який використовується для побудови мереж Інтернету речей на великі відстані (Long Range Wide Area Network)
LPWAN	Енергоефективна мережа дальнього радіусу дії (Low-power wide-area network)
MAC-адреса	Унікальний ідентифікатор, що зіставляється з різними типами устаткування для комп'ютерних мереж (Media Access Control)
MQTT	Спрощений мережевий протокол, що працює на TCP/IP (Message Queue Telemetry Transport)
NIST	Національний інститут стандартів і технології (National Institute of Standards and Technology)
PaaS	Платформа як послуга (Platform as a Service)
PAN	Персональна мережа (Personal Area Network)
RFID	Радіочастотна ідентифікація (Radio Frequency Identification)
RSA	Криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел (Rivest-Shamir-Adleman)

SaaS	Програмне забезпечення як послуга (Software as a service)
SCADA	Диспетчерське управління і збір даних (Supervisory Control And Data Acquisition)
SNA	Системна мережева архітектура (Systems Network Architecture)
SNMP	Простий протокол керування мережею (Simple Network Management Protocol)
STP	Рівень провадження розумних технологій (Smart Technology Penetration)
TCP/IP	Набір протоколів мережі Інтернет (Transmission Control Protocol/Internet Protocol)
TLS	Захист на транспортному рівні (Transport Layer Security)
VPN	Віртуальна приватна мережа (Virtual private network)
WAN	Глобальна мережа (Wide area network)
Wi-Fi	Технологія бездротового доступу до інтернету (Wireless Fidelity)
АЦП	Аналого-цифровий перетворювач
ІКТ	Інформаційно-комунікаційні технології
ПЗ	Програмне забезпечення

ВСТУП

Закон України «Про Національну програму інформатизації» [1] визначає пріоритети держави в області просування електронних інформаційних ресурсів. Основною метою є підвищення ефективності вітчизняного виробництва через застосування інформаційно-комунікаційних та цифрових технологій. В рамках цієї стратегії важлива роль належить електронним комунікаціям, які розглядаються як ключовий елемент впровадження електронних інформаційних ресурсів у суспільне життя.

Закон України «Про електронні комунікації» [2] встановлює технічні основи для мереж електронних комунікацій. Зокрема, він визначає електронну комунікаційну мережу як комплекс технічних засобів і споруд, призначених для надання електронних комунікаційних послуг, а також наголошує на важливості їх інфраструктури — технічних засобів і споруд, які забезпечують роботу таких мереж.

Отже, обидва закони формують законодавчу базу для розвитку цифрової інфраструктури і впровадження електронних сервісів в Україні.

Міністерство цифрової трансформації України [3] затвердило конкретні критерії класифікації електронних комунікаційних мереж за швидкісними параметрами — мережі широкосмугового доступу, високошвидкісні, а також мережі високої і надвисокої пропускної здатності. Це дозволяє систематизувати мережеву інфраструктуру та забезпечує більш точний аналіз її можливостей.

У свою чергу, закон України «Про захист інформації в інформаційно-комунікаційних системах» [4] наголошує на важливості захисту інформації. Цей захист направлений на забезпечення цілісності, конфіденційності та доступності даних у системах, що є фундаментальним для безпечного функціонування інформаційних технологій.

Отже, наведені документи та технології формують основу, забезпечуючи класифікацію, безпеку та застосування інновацій в Україні.

Важливим сучасним напрямом для сучасного цифрового розвитку є використання технологій Інтернету речей (IoT). Це мережа, яка об'єднує

фізичні пристрої і об'єкти, обладнані датчиками та програмним забезпеченням для збору, обробки та обміну даними. IoT розширює можливості автоматизації, оптимізації виробництва і вирішення побутових та суспільних завдань завдяки мережевому підключенню таких пристроїв [5,6].

Пристрої Інтернету речей (IoT), або «розумні об’єкти», охоплюють широкий спектр — від простих пристроїв розумного дому до складного промислового обладнання й транспортних систем. Ця технологія відкриває можливості для формування «розумних міст», де IoT-структури використовуються для підвищення ефективності управління міським середовищем і покращення життя мешканців.

Станом на сьогодні у світі налічується близько 18.8 мільярдів IoT-пристроїв, і ця кількість постійно зростає [7].

Таким чином технології IoT стають невід’ємною частиною цифрової трансформації, дозволяючи побудувати інтелектуальні системи для багатьох сфер життя і виробництва.

При цьому методів підвищення ефективності мереж IoT слід віднести:

- Створення відповідної мережевої інфраструктури, максимально адаптованої до потреб технологій IoT. Виміром ефективності в цьому випадку є спрощення доступу до об’єктів IoT при організації їх функціонування в загальній інформаційній мережі.

- Збільшення продуктивності каналів передавання інформації в мережевій інфраструктурі за рахунок використання сучасних і перспективних, зокрема, оптоволоконних, технологій. Виміром ефективності в цьому випадку є збільшення кількості об’єктів IoT в специфічній IoT-інфраструктурі та прискорення їх реакції.

- Вдосконалення технологій безпроводового доступу до об’єктів IoT в загальній інформаційній мережі (технології 5G, 6G), а також в специфічній IoT-інфраструктурі (відповідно до діючих стандартів IoT-безпроводових технологій).

Виміром ефективності в цьому випадку є збільшення кількості об’єктів IoT в специфічній IoT-інфраструктурі та прискорення їх реакції.

- Використання технологій хмарних технологій при використанні об’єктів IoT в специфічній IoT-інфраструктурі. Виміром ефективності в цьому випадку є прискорення реакції об’єктів IoT та раціональне використання ресурсів мереж IoT [8].

- Використання технологій кіберзахисту мереж IoT. Виміром ефективності в цьому випадку є захист об’єктів IoT в специфічній IoT-інфраструктурі від зовнішніх небажаних втручань [9].

Для реалізації Концепція ефективності необхідними елементами вивчення та відображення в роботі є:

- Формулювання мети, об’єкту дослідження, завдань дослідження.

- Аналіз діючих мережевих технологій і відповідних стандартів організації специфічній IoT-інфраструктурі, зокрема, безпроводових технологій доступу до об’єктів IoT.

- Огляд практики використання хмарних технологій та забезпечення кібербезпеки при реалізації мереж IoT.

- Формулювання критеріїв ефективності та обґрунтування інструментів її підвищення за відповідних умов.

- Формулювання пропозицій щодо підвищення ефективності мереж IoT в сучасних умовах і в перспективних інформаційних системах загального користування.

Метою роботи є дослідження та аналіз інтеграції технології Інтернету речей (IoT) з мережевими, зокрема, безпроводовими технологіями, у сполученні із хмарними та безпековими технологіями, аналіз переваг та викликів їх інтеграції та перспективи подальшого розвитку для визначення ключових методів підвищення ефективності мереж Інтернету речей.

Об’єктом дослідження є мережеві, зокрема, безпроводові технології у взаємодії з хмарними та безпековими технологіями в структурі IoT.

Предмет дослідження: Характеристики, можливості, вразливості та сценарії застосування сучасних мережних технологій і протоколів для забезпечення ефективної, безпечної та надійної взаємодії пристроїв IoT.

1. АНАЛІЗ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ ТА СКЛАДОВИХ, ЯКІ ЗАБЕЗПЕЧУЮТЬ ЇЇ РЕАЛІЗАЦІЮ.

1.1. Концепція Інтернету речей

Інтернет речей (англ. Internet of Things, IoT) — це ідея створення глобальної інфраструктури, яка об'єднує фізичні об'єкти в єдину мережу через Інтернет або інші мережеві технології. Суть полягає в тому, що навіть прості предмети, такі як домашні пристрої, автомобілі, промислове обладнання чи біосенсори, можуть бути оснащені електронними компонентами, які збирають, обробляють і передають інформацію. Таким чином, речі стають активними учасниками цифрового середовища — не лише джерелами даних, а й автономними учасниками взаємодії.

Концепція IoT сформувалась поступово, на стику розвитку кількох технологічних напрямів — сенсорики, мікроелектроніки, бездротового зв’язку та хмарних обчислень. Поєднання цих технологій створило інтелектуальні об’єкти, здатні обмінюватися інформацією без участі людини. Наприклад, «розумний» термостат не тільки заміряє температуру, а й аналізує її та управляє системою опалення автоматично [10].

Автоматизація є однією з ключових характеристик IoT: передача і обробка інформації виконуються безперервно і без суттєвого втручання людини або зовсім без нього. Це відкриває можливості для впровадження складних сценаріїв моніторингу, реагування та оптимізації в реальному часі. Так, в «розумному місті» система керування трафіком може змінювати сигнали світлофорів на основі даних із датчиків руху, зменшуючи затори та час простою автотранспорту.

Крім того, IoT відзначається високою масштабованістю. Налаштована система може розширюватися майже необмежено — додаючи нові пристрої, сервіси або типи даних. Це особливо актуально в промисловості, де кількість сенсорів може досягати десятків тисяч, що робить критичним питання стандартизації обміну даними та сумісності пристроїв різних виробників.

Поняття IoT передбачає не лише фізичне підключення пристроїв, а й їхню логічну взаємодію: сенсори генерують дані, які потім аналізуються, зберігаються чи використовуються для ухвалення рішень. Таким чином, IoT виступає як міст між фізичним і цифровим світами.

Сьогодні IoT знаходить застосування в багатьох сферах. У побуті — це автоматизація житла, охорона та енергозбереження. В медицині — віддалений моніторинг пацієнтів і в реальному часі. В промисловості — контроль стану обладнання, телеметрія, обслуговування об'єктів [11].

За останні роки технології Інтернету речей стали одніми з провідних технологій завдяки розвитку її складових:

– розвиток бездротового зв’язку, що забезпечує передачу даних від сенсорів до хмар і пристроїв через Інтернет (Wi-Fi, Bluetooth, стільниковий зв’язок, Zigbee, LoRaWAN);

– поява доступних та енергоефективних сенсорів і приводів, які складають основу IoT-пристроїв, дозволяючи машинам взаємодіяти з фізичним світом без участі людини;

– хмарні обчислення, які розширюють можливості IoT, забезпечуючи зберігання, обробку та аналіз великих обсягів даних та надають інструменти для створення і розгортання IoT-додатків;

– інструменти Big Data аналітики, що дають змогу ефективно аналізувати великі дані за допомогою машинного навчання, візуалізації та прогнозування поведінки споживачів.

1.1.1. Технології, що роблять Інтернет речей можливим

Для реалізації Інтернету речей об’єднується низка технологій [6]:

- **Датчики та виконавчі механізми**: Датчики — пристрої, що реєструють зміни у довкіл, як температура, вологість, освітлення, рух чи тиск. Виконавчі механізми — пристрої, що здатні фізично впливати на навколишнє середовище, наприклад, відкривати чи закривати клапан або вмикати двигун. Ці компоненти є основою IoT, адже дають змогу машинам і пристроям

взаємодіяти з фізичним світом і впроваджувати автоматизацію без участі людини.

- **Технології підключення**: Для передачі даних від датчиків і виконавчих механізмів до хмарних сервісів і інших IoT-пристроїв потрібно забезпечити з'єднання з Інтернетом. Використовуються різноманітні бездротові технології, такі як Wi-Fi, Bluetooth, стільниковий зв'язок, Zigbee та LoRaWAN.
- **Хмарні обчислення**: Хмара — це середовище для зберігання, обробки та аналізу величезних обсягів даних, створених IoT-пристроями. Хмарні платформи надають інструменти та інфраструктуру для роботи з такими обсягами, а також допомагають розгорнути IoT-додатки.
- **Аналіз великих даних**: Щоб розуміти та використовувати величезні дані, що надходять від IoT, підприємства застосовують передові інструменти аналітики, такі як алгоритми машинного навчання, візуалізацію та прогнозування поведінки споживачів, трендів ринку.
- **Технології безпеки та конфіденційності**: З поширенням IoT зростає потреба у захисті пристроїв і їхніх даних. Застосовуються методи шифрування, контроль доступу і системи виявлення вторгнень для захисту від кібератак.

1.1.2. Сфери застосування IoT.

Технології Інтернету речей впроваджуються у багатьох галузях, створюючи нові бізнес-моделі і підвищуючи ефективність існуючих процесів [12]. IoT можна адаптувати під специфіку різних сфер. Основні напрямки використання технологій Інтернету речей надано на рис. 1.1 [13].

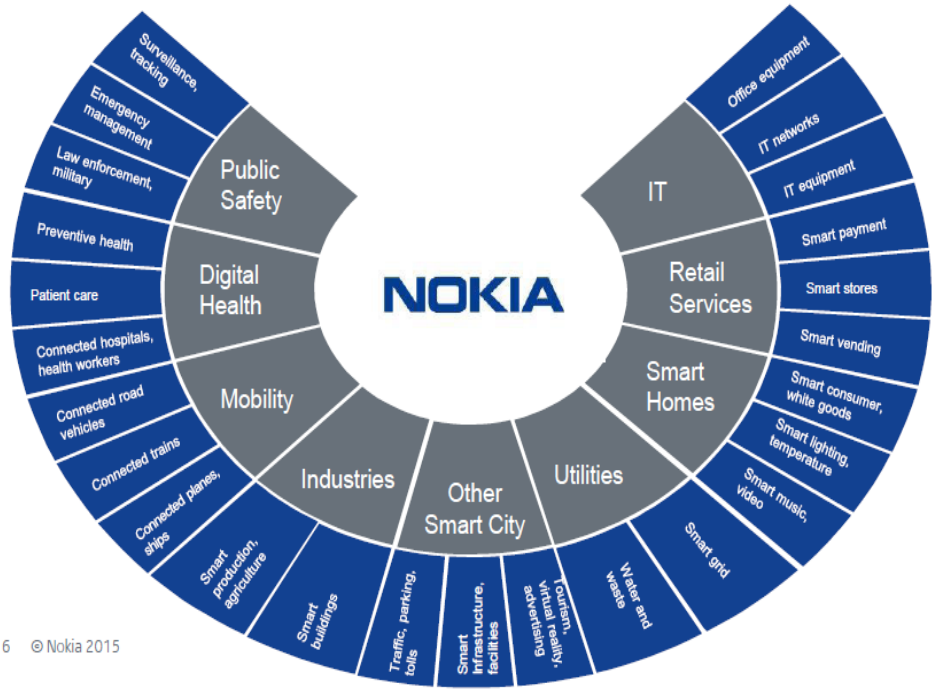

Рисунок 1.1 – Основні напрямки використання технологій Інтернету речей

- **Охорона здоров'я (Healthcare)**: Носимі пристрої (фітнес-трекери, смарт-годинники) і медичні сенсори дозволяють дистанційно контролювати параметри пацієнтів (пульс, тиск, рівень глюкози), що допомагає у ранній діагностиці та персоналізованому лікуванні. Системи "розумної лікарні" оптимізують управління обладнанням і ресурсами.
- **Розумні будинки (Smart Homes)**: IoT автоматизує керування освітленням, кліматом (розумні термостати), безпекою (датчики руху, розумні замки), побутовою технікою (холодильники, кавоварки), що підвищує комфорт, безпеку та енергоефективність свого житла.
- **Розумні міста (Smart Cities)**: IoT допомагає оптимізувати міську інфраструктуру: управління трафіком (розумні світлофори, паркування), моніторинг якості повітря і шуму, ефективне керування водопостачанням, енергоспоживанням і вивозом сміття.
- **Промисловість (Industry, IIoT)**: Застосовується для моніторингу обладнання (прогнозне обслуговування), оптимізації виробничих процесів, управління логістикою та безпеки праці.

- **Енергетика (Smart Grid)**: IoT дозволяє створювати "розумні" електромережі з ефективним розподілом енергії, моніторингом в реальному часі, інтеграцією відновлюваних джерел і швидким реагуванням на аварії.
- **Сільське господарство (Agriculture)**: "Розумне фермерство" використовує IoT-сенсори для моніторингу стану ґрунту, вологості, температури, здоров'я тварин, що оптимізує полив, внесення добрив, прогнозує врожайність.
- **Транспорт та логістика (Transport)**: IoT забезпечує моніторинг руху транспортних засобів, оптимізацію маршрутів та відстеження вантажів, підвищуючи безпеку і ефективність перевезень.
- **Роздрібна торгівля (Retail)**: Використання IoT для моніторингу поведінки покупців, контролю запасів, відстеження відправлень та оптимізації роботи магазинів.

Такий перелік застосувань не є вичерпним — IoT активно проникає у екологічний моніторинг, безпеку, освіту та інші сфери, підтверджуючи свою універсальність і великий потенціал впливу.

1.2. Архітектура технології Інтернету речей

Архітектура IoT — це структура, яка визначає, як взаємодіють різні компоненти Інтернету речей: сенсори, приводи, мережі та додатки IoT-середовища. Зазвичай вона складається з кількох рівнів і складових, кожен із яких виконує свою функцію — від фізичних пристроїв збору даних до мережевих компонентів і IoT-платформ для обробки та зберігання.

Хоча універсального стандарту немає, існує узагальнена еталонна архітектура, рекомендована ITU-T Y.2060, що містить чотири рівні (рис. 1.2) [14]:

- Рівень IoT-пристроїв
- Рівень мережі
- Рівень сервісної та програмної підтримки
- Рівень додатків

Рисунок 1.2 демонструє цю структуру [15].

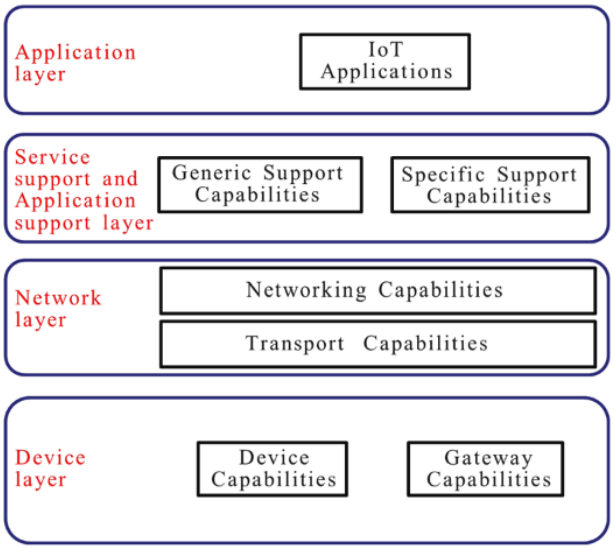

Рисунок 1.2 – 4-рівнева архітектура IoT

За стандартами ITU-T і IEEE (Standard for an Architectural Framework for the Internet of Things) можна виокремити більш детальну 7-рівневу архітектуру IoT (рис. 1.3), що охоплює: сенсори, приводи, мережі зв'язку, шлюзи IoT, додатки, менеджмент і безпеку [16-17].

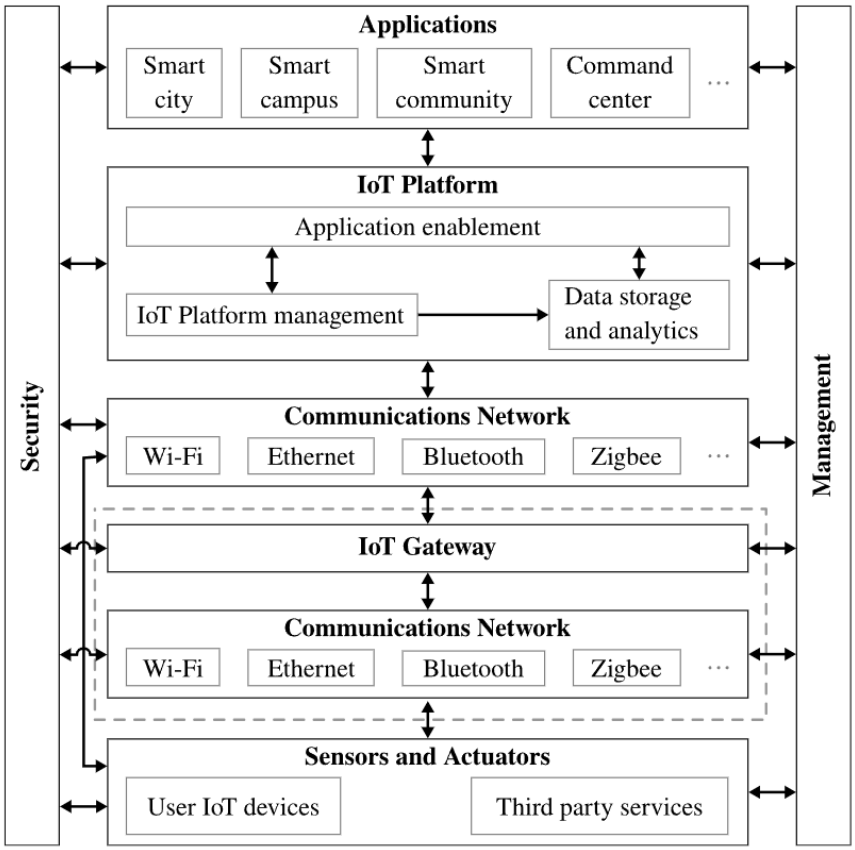

Рисунок 1.3 – 7-рівнева архітектура IoT

1.2.1. Порівняльний аналіз архітектурних моделей IoT

Вибір архітектурної моделі впливає на складність проєктування, апаратні та програмні вимоги, масштабованість, інтеграцію з хмарними платформами та аналітикою, а також організацію безпеки. Таблиця 1.1 порівнює основні параметри 4-рівневої та 7-рівневої моделей [18-20].

Таблиця 1.1 – Порівняння архітектурних моделей IoT за ключовими критеріями.

Критерій	4-рівнева модель	7-рівнева модель
Призначення	Чітко розділяє рівні обробки між мережею і додатками	Деталізований розподіл функцій від пристроїв до бізнес-процесів
Складність реалізації	Середня	Дуже висока
Масштабованість	Задовільна, частину обробки можна винести в хмару	Максимальна, дозволяє масштабувати домени незалежно
Придатність до критичних застосувань	Для середніх рішень, базова автоматизація	Для великих промислових і корпоративних екосистем
Модель посилань / стандарти	Відповідає IoT-моделі ITU-T Y.2060	Відповідає Cisco IoT Reference Model
Можливості безпеки	Легше захищати транспорт і обробку	Підтримує багаторівневу безпеку з різними механізмами

1.2.2 Порівняльний аналіз компонент 7-рівневої архітектурної моделі IoT

Окремі рівні 7-рівневої архітектури IoT мають такі особливості [18-20]:

1. **Рівень IoT-пристроїв**: містить сенсори (апаратні пристрої для збору параметрів довкілля) та приводи (виконують команди, наприклад, включають або вимикають пристрої).

2. **Рівень мережі**: забезпечує зв’язок і передачу даних від пристроїв до IoT-шлюзу та платформи через різні протоколи (Wi-Fi, Ethernet,, Zigbee тощо).

3. **Рівень IoT-шлюзу**: з'єднує різні мережі, стандарти протоколів рівня даних та формати з платформою IoT, дозволяючи працювати з різнотипними пристроями, які можуть використовувати різні протоколи.

4. **Рівень IoT-платформи**: центральна система управління та контролю пристроями, що забезпечує:

- менеджмент акаунтів, інтеграцію і керування пристроями, управління даними та системою,
- зберігання і обробку даних,
- підтримку застосунків.

5. **Рівень застосунків**: це програмне забезпечення з графічним інтерфейсом і аналітикою, що дає змогу користувачам контролювати і взаємодіяти з IoT-пристроями.

6. **Рівень безпеки**: відповідає за захист конфіденційності, цілісності і доступності даних — аутентифікація, контроль доступу, моніторинг і аудит.

7. **Рівень менеджменту**: здійснює загальне управління системою — моніторинг, конфігурування, оновлення пристроїв, управління продуктивністю і мережею.

1.3. Архітектура мережі IoT.

1.3.1. Мережева архітектура систем IoT та її особливості

Визначення IoT згідно з рекомендацією ITU-T Y.2060 описує Інтернет речей як глобальну інформаційну інфраструктуру, що забезпечує передові послуги через організацію зв’язку між речами — фізичними або віртуальними — із застосуванням існуючих та нових інформаційних і комунікаційних технологій [21]. Під «річчю» мається на увазі фізичний об’єкт або його віртуальний аналог, ідентифіковані та об'єднані в мережу.

Під «пристроєм» розуміють обладнання, що має можливості комунікації, та часто сенсори, актуатори, збір, обробку і зберігання інформації. Пріоритет віддається пристроям, які збирають інформацію та розповсюджують її через різні мережеві способи — із шлюзами, без них, або прямо між собою.

Рекомендація Y.2060 передбачає різні способи організації з’єднань: глобальні мережі, локальні, безпроводові ad-hoc та mesh мережі. Вони забезпечують передачу даних від пристроїв до додатків та керування командами від програм до пристроїв (рис. 1.4).

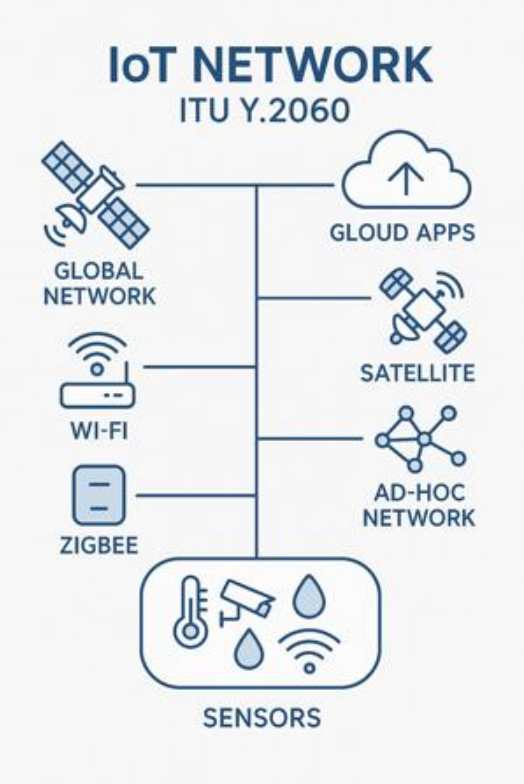

Рисунок 1.4. — Схема IoT-мереж за стандартом Y.2060 [21]

Формально Інтернет речей складають сенсори, дані, мережі й послуги:

IoT = Сенсори + Дані + Мережі + Послуги.

IoT — це сукупність багатьох приладів і пристроїв, об’єднаних через різні канали та протоколи у глобальну мережу, якою часто виступає Інтернет за протоколом IP. IoT реалізує різноманітні "smart" додатки у побуті, медицині, промисловості та інших сферах [22].

Проекти IoT не мають універсального підходу, але можна виокремити основні будівельні блоки архітектури з урахуванням масштабованості та гнучкості. Наприклад, PNN Soft пропонує гнучкі схеми даних для зберігання безперервно зростаючих інформаційних потоків.

1.3.2. Призначення інфокомунікаційної мережі

Під час звернення користувача до онлайн-сервісів зі своїх гаджетів, ці сервіси фізично знаходяться далеко. Завдяки інфокомунікаційним мережам запити передаються через низку мережевих пристроїв — маршрутизатори, комутатори, сервери — забезпечуючи зв’язок.

Інформатизація — комплекс заходів (організаційних, правових, технічних, економічних), які створюють умови для переходу до інформаційного суспільства з цифровими технологіями. «Засоби інформатизації» — це будь-які технологічні ресурси (комп’ютери, програмне забезпечення, мережі), призначені для збору, обробки, зберігання й передачі даних [1].

Інфокомунікаційна мережа — ключовий інструмент інформатизації, що об'єднує розподілені сервери, бази даних, програми і кінцеві пристрої у спільну інфраструктуру. Вона забезпечує передачу сигналів із їх обробкою (маршрутизація, кодування) [4].

Рисунок 1.5 ілюструє схему інфокомунікаційної мережі з кінцевими пунктами, каналами зв’язку і вузлами [23].

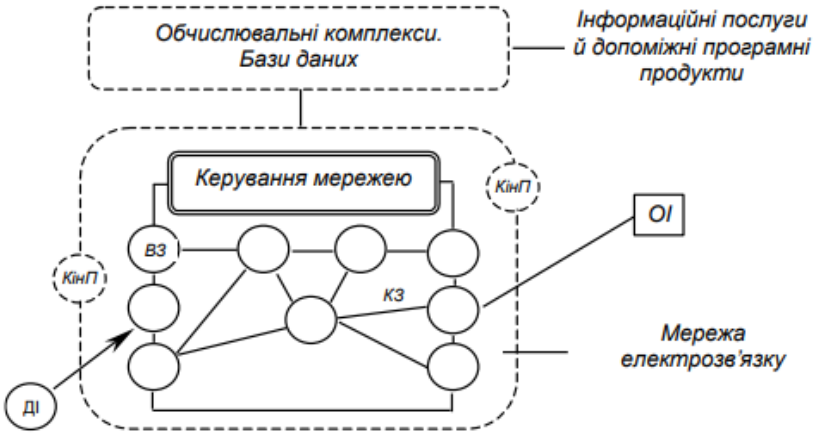

Рисунок 1.5. Схема інфокомунікаційної мережі:
КінП (Кінцевий пункт), КЗ (Канал зв’язку), ВЗ (Вузол зв’язку),
ДІ (Джерело інформації), ОІ (Одержувач інформації)

1.3.3. Вимоги до інфокомунікаційних мереж

Сучасні мережі повинні підтримувати різні сервіси — від веб-серфінгу до потокового відео і VoIP-дзвінків; вони мають працювати з різними фізичними середовищами (оптоволокно, кручена пара, радіохвилі) і типами обладнання (комутатори, маршрутизатори, точки доступу).

Основні вимоги:

- **Відмовостійкість**: мережа має залишатися працездатною навіть при виході з ладу окремих елементів, забезпечуючи альтернативні маршрути (пакетообмін — перенаправлення пакетів у разі недоступності маршруту);
- **Масштабованість**: легке розширення мережі без погіршення якості завдяки стандартам, що забезпечують сумісність нових пристроїв;
- **Якість обслуговування (QoS)**: пріоритетність трафіку для голосу, відео, інших додатків з параметрами — затримка, джиттер, втрата пакетів, пропускна здатність. Закон України «Про електронні комунікації» встановлює обов'язки провайдерів щодо якості послуг і звітності про чинники, що впливають на якість [2];
- **Безпека**: захист фізичної інфраструктури і інформації (шифрування, автентифікація, контроль доступу), оскільки порушення безпеки може призвести до збоїв, витоку даних і фінансових втрат. Безпека розглядається як трикутник із конфіденційності, цілісності і доступності [24].

1.4. Застосування хмарних технологій в IoT

Термін «хмара» описує окреме IT-середовище для віддаленого надання масштабованих ресурсів. Перш ніж хмарні обчислення стали окремим сегментом IT, символ хмари використовувався для позначення Інтернету в різних технічних специфікаціях та документації веб-архітектури [25].

Впровадження хмарних технологій розширює функціонал IoT-пристроїв, забезпечуючи ефективне управління, обробку та аналіз даних у реальному часі.

Особливості використання хмарних технологій у IoT [26]:

- Центральна платформа з практично необмеженими обчислювальними ресурсами для зберігання та обробки великих обсягів даних, що генеруються IoT-пристроями.
- Реальне управління даними з IoT у режимі реального часу, що дозволяє знизити витрати на обробку.

- Віддалений моніторинг стану та керування IoT-пристроями через веб-інтерфейси або мобільні застосунки.
- Віддалене оновлення програмного забезпечення, що підвищує безпеку й функціональність пристроїв.
- Використання штучного інтелекту і машинного навчання для аналітики широких даних, що зберігаються в хмарі.

Приклади застосування [26]:

- В медицині — віддалений моніторинг пацієнтів через IoT-пристрої, що передають дані в хмару для аналізу.
- У промисловості — моніторинг обладнання й прогнозування несправностей у реальному часі.
- У «розумних містах» — керування трафіком, якістю повітря, освітленням.
- У «розумних будинках» — контроль побутових пристроїв, безпеки і моніторинг повітря через Wi-Fi чи Bluetooth з використанням голосових помічників (Amazon Alexa, Google Home).

1.4.1. Переваги хмарних технологій

- **Зниження витрат**: хмарні технології пропонують масштабоване зберігання і обробку з оплатою за фактичне використання послуг («pay-per-usage»), позбавляючи організації витрат на потужне локальне обладнання.
- **Автоматичні оновлення**: можливість віддаленого оновлення ПЗ підвищує безпеку і знижує витрати на технічне обслуговування.
- **Висока продуктивність і гнучкість**: хмари дають майже необмежені ресурси, швидко масштабуються під навантаження, ідеальні для обробки великих даних.
- **Безпека даних**: постачальник послуг забезпечує резервне копіювання даних і зберігання в різних місцях для зниження ризику втрати.
- **Доступність**: дані доступні в реальному часі із будь-якого пристрою з підключенням до Інтернету.

1.4.2. Складнощі застосування хмарних технологій в IoT

Основні виклики щодо застосування хмарних технологій в IoT:

- Забезпечення безпеки і конфіденційності, особливо через бездротову передачу даних, що створює ризики атак (DDoS, MITM).
- Відповідність законодавству (HIPAA, GDPR) вимагає надійних підходів для інтеграції периферійних комунікацій і хмарних сервісів із пріоритетом безпеки [28][29].
- Надійність мережі: оскільки дані і додатки можуть зберігатися в різних місцях, затримки мережі, слабкий сигнал або перевантаження можуть призводити до проблем, що особливо важливо для чутливих сценаріїв (медмоніторинг).
- Використання периферійних обчислень (edge computing) допомагає знизити затримки та навантаження мережі.
- Складність інтеграції через унікальне обладнання, прошивку, протоколи різних пристроїв потребує розробки складного проміжного ПЗ, підвищує ризики несправностей.
- Високі початкові інвестиції (особливо для великих організацій з безпековими вимогами) можуть бути бар’єром для переходу.

1.5 Проблеми безпеки та конфіденційності IoT

Загрози в IoT-архітектурі варто розглядати по рівнях, оскільки атаки можуть порушувати доступність, цілісність та конфіденційність даних, а також фізичну і функціональну безпеку кіберфізичних систем. Для захисту застосовується багаторівнева вбудована система безпеки з легкою криптографією, автентифікацією, авторизацією, сегментацією мережі, моніторингом аномалій і безпечним управлінням життєвим циклом пристроїв [30].

- **Рівень пристроїв**: поширені атаки включають клонування або підміну сенсорів, фальсифікацію даних, фізичний саботаж, side-channel атаки, завантаження неавторизованої прошивки, а також використання вузла як платформи для проникнення в мережу. Це пов’язано зі слабкою

автентифікацією, відкритими debug-інтерфейсами, відсутністю захисту пам’яті та оновлення ПЗ.

- **Мережевий рівень**: атаки включають перехоплення і зміну трафіку (MitM), заміну вузлів, DoS/DDoS атаки на шлюзи чи хмарні сервіси, порт-сканування та експлуатацію вразливих протоколів (ZigBee, OT). Особливу небезпеку становить конвергенція IT та OT, коли компрометація IT-мережі дає доступ до виробничих систем через слабкі IoT-вузли.
- **Сервісний та додатків рівень**: можливі загрози компрометації API, підробки команд, ескалації привілеїв, уразливості веб-інтерфейсів, витоки телеметрії. Особливо критична функціональна безпека — маніпуляції віртуальними даними можуть викликати фізичну шкоду.

Основні вимоги безпеки, які мають виконуватися на всіх рівнях IoT — це автентифікація користувачів, управління ідентичностями, захищений обмін даними, безпечна мережа, сховище, виконання програм, захист контенту і стійкість до несанкціонованого доступу. На рисунку 1.6 узагальнено основні напрями загроз безпеки та конфіденційності в IoT.

Рисунок 1.6 – Основні напрями загроз безпеки та конфіденційності в IoT.

Основні аспекти забезпечення безпеки в технологіях Інтернету речей [30]:

- Ідентифікація користувача: автентифікація за ключем чи паролем перед доступом до ресурсів.

- Керування ідентичністю: позначає і контролює доступ пристроїв до системи, пов’язуючи права користувачів із розпізнаними сутностями.
- Забезпечення безпечного обміну даними: автентифікація зв’язку, схоронність і цілісність переданих даних.
- Безпечна мережа: дозвіл доступу лише авторизованим пристроям.
- Захищене зберігання: запобігання несанкціонованому доступу до даних.
- Безпечне середовище виконання програм: захист від небажаних програм.
- Безпека контенту: захист інформації від вірусів і зловмисників.
- Захист від маніпуляцій: механізми для запобігання несанкціонованому доступу до системи.

Відповідь на ці загрози реалізується вбудованою системою безпеки IoT із збором інформації з датчиків, аналізом контексту і превентивними діями в мережевій архітектурі.

Ключові рішення включають застосування легкої криптографії, безпечної ОС із захищеним завантаженням і контролем цілісності, а також фізичний захист (апаратні ключі, антиманіпуляційні корпуси).

Безпечна IoT-платформа підтримує захищені сховища, ізольоване виконання програм і контроль доступу до пам’яті — формуючи ціліс архітектуру безпеки від сенсора до хмарного застосунку.

Висновки до розділу 1

У першому розділі детально розглянуто концепцію Інтернету речей, складові технології, що забезпечують її реалізацію: телекомунікаційні мережі, хмарні технології, засоби захисту інформації та їхню інтеграцію. Проаналізовано переваги та недоліки інтеграції різних складових, описано 7-рівневу архітектуру IoT та представлені моделі розгортання (публічна, приватна, гібридна).

Обґрунтовано висновок, що мережеві технології виступають фундаментальною інфраструктурою, яка підвищує ефективність застосування IoT-пристроїв.

Ключовою частиною розділу став аналіз інтеграції мережних технологій з іншими складовими IoT. Розглянуто принципи їх спільної роботи, що показало роль транспортної телекомунікаційної мережі як основи для гарантованого зберігання, обробки і аналізу даних, згенерованих IoT-пристроями.

Визначено переваги і складнощі такої інтеграції, а також наведено опис основних платформ IoT та їх принципів роботи.

2. ПОРІВНЯННЯ МЕРЕЖЕВИХ ТЕХНОЛОГІЙ, ЯКІ ЗАБЕЗПЕЧУЮТЬ ФУНКЦІОНУВАННЯ IOT

Основою IoT-технології є передача керуючої та виконавчої інформації через інтернет-мережі. І сам Інтернет функціонує в межах інфраструктури мереж електронних комунікацій. Тому важливо порівняти мережеві технології, що забезпечують роботу IoT.

2.1. Загальна характеристика комунікаційної мережі.

За ознакою покриття території і технічними особливостями мережі поділяються на:

- **LAN (Local Area Network)**: покриває територію до 1-1,5 км (офіси, будівлі). Технології: Ethernet (100 Мбіт/с – 10 Гбіт/с), Wi-Fi (до 9,6 Гбіт/с у Wi-Fi 6). Характеристика: адмініструється однією організацією, низькі затримки (до 1 мс), висока пропускна здатність.
- **MAN (Metropolitan Area Network)**: покриває місто або регіон до 50-60 км. Технології: оптоволоконні DWDM, маршрутизатори з MPLS, Ethernet OAM. Характеристика: об’єднує LAN-мережі, пропускна здатність від 100 Мбіт/с до кількох Гбіт/с.
- **WAN (Wide Area Network)**: територія від сотень до тисяч кілометрів (міжрегіональні, міждержавні). Технології: PDH/SDH, IP/MPLS по оптиці, 4G/5G бекхаул. Характеристика: нижча пропускна здатність і вища латентність (30-300 мс), управління кількома провайдерами.

2.1.1. Класифікація мереж електронних комунікацій за ознакою пропускної здатності

В Україні, згідно наказу Міністерства цифрової трансформації [3], мережі поділяються:

- **Широкосмугова (Broadband)**: Downlink ≥2 Мбіт/с, Uplink ≥0.5 Мбіт/с, поширена серед користувачів дому та малого бізнесу.

- **Високошвидкісна (High-Speed)**: фіксований зв'язок ≥30 Мбіт/с (VDSL2, LTE-Advanced); мобільний — Downlink ≥15 Мбіт/с, Uplink ≥3 Мбіт/с.
- **Мережа високої пропускної здатності (High Throughput)**: фіксований — Downlink ≥100 Мбіт/с (GPON, XGS-PON, Ethernet 1 Гбіт/с), мобільний — Downlink ≥50 Мбіт/с.
- **Мережа надвисокої пропускної здатності (Ultra-High Throughput)**: фіксований — Downlink ≥1 Гбіт/с (XGS-PON, 10 Gigabit Ethernet), мобільний — Downlink ≥150 Мбіт/с (5G SA, mmWave).

Вимоги до якості послуг примушують провайдерів гарантувати мінімальну швидкість для різних сервісів [31,32].

2.1.2. Компоненти інфокомунікаційної мережі

Сучасна мережа складається з апаратних та програмних компонентів [33,34].

2.1.2.1. Апаратні компоненти та середовище передачі

Кінцеве обладнання (термінальні пристрої): користувацькі пристрої (ПК, ноутбуки, смартфони, планшети), принтери, сервери, що мають унікальні адреси (IP, MAC) для ідентифікації та прийому даних

Рисунок 2.1. Кінцеві пристрої мережі: ПК, ноутбук, сервер, смартфон, планшет

Проміжні мережеві пристрої, які об’єднують кінцеві пристрої в єдину інфраструктуру, виконують маршрутизацію, фільтрацію і ретрансляцію сигналів:

– Комутатори (Switch) і точки доступу (Access Point) працюють на канальному рівні (LAN/WLAN).

– Маршрутизатори (Router) відповідають за маршрутизацію IP-пакетів між мережами.

– Міжмережеві екрани (Firewall) захищають мережу, фільтруючи трафік.

Рисунок 2.2. Проміжні мережеві пристрої: комутатор, точка доступу, маршрутизатор, міжмережевий екран (пристрої безпеки)

Функції проміжних пристроїв включають регенерацію сигналів, підтримку топології (Routing Table, Spanning Tree), інформування про помилки (ICMP), резервні маршрути, пріоритизацію трафіку (QoS), безпекові політики (ACL, Stateful Inspection) [24].

Середовище передачі даних — фізичні середовища, через які передається інформація між пристроями. Можуть бути:

- **Кабельні** (закриті), як:
  - Кручена пара (UTP, STP) — найбільш поширене для LAN (Ethernet).
  - Коаксіальний кабель — раніше для 10BASE-2/10BASE-5.
  - Оптоволокно — для магістральних і міжміських каналів (пропускна здатність до сотень Гбіт/с).
- **Безпроводові** (відкриті), як:
  - Радіохвилі (Wi-Fi, Bluetooth, Zigbee, LoRa, NB-IoT).
  - Інфрачервоні (IR) — менш поширені, потребують прямої видимості.
- **Супутникові** — для віддалених регіонів, дорожчі, із більшими затримками, але майже планетарне покриття.

У провідному середовищі інформація передається у вигляді електричних імпульсів, які кодують біти за певними стандартами (наприклад, NRZ,

Manchester) для відновлення початкового сигналу на приймальній стороні. В оптоволоконних лініях передача здійснюється за допомогою світлових імпульсів від лазера або LED. У радіозв'язку інформація передається через електромагнітні хвилі, які модулюються різними способами (FSK, PSK, QAM тощо).

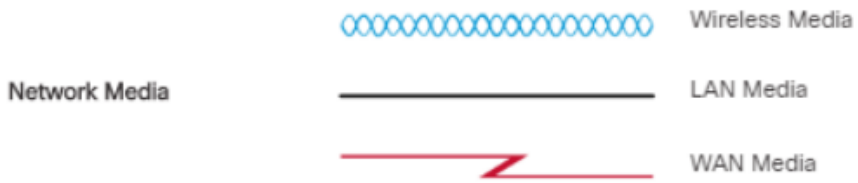

Рисунок 2.3. Середовище передачі даних: Кручена пара, оптоволокно, радіохвилі, супутниковий канал

2.1.2.2. Широкосмуговий інтернет та його технології

Широкосмуговий інтернет — доступ із достатньою швидкістю для HD-відео, онлайн-ігор, відеоконференцій [31].

Основні технології:

- **xDSL** (працює по крученої парі):
  - ADSL2+: швидкість до 24 Мбіт/с завантаження, 1.4 Мбіт/с віддачі, відстань до 5 км.
  - VDSL2: до 100 Мбіт/с (до 1 км).
  - HDSL/SDSL: симетричні лінії по 2 Мбіт/с (офісні).
- **DOCSIS**: передача інтернету по коаксіальних кабелях, часто до сотень Мбіт/с, кабельні провайдери.
- **FTTH** (Fiber-to-the-Home): оптоволокно до квартири або будинку з швидкістю до 1 Гбіт/с і вище (GPON, XGS-PON).
- **FTTB** (Fiber-to-the-Building): оптоволокно до будівлі, далі UTP або оптоволокно всередині, швидкості 100-1000 Мбіт/с.
- **FTTC / FTTCabinet** (Fiber-to-the-Cabinet): волокно до шафи, далі DSLAM із VDSL2 до користувача по витій парі.

- **FTTN** (Fiber-to-the-Node): волокно до Node (вуличний розподільник), далі мідь до будинків, швидкість змінюється залежно від відстані.
- **GPON** (Gigabit PON)

Пасивна мережа, що використовує сплітери з розподілом 1:32 або 1:64, забезпечує швидкість до 2,5 Гбіт/с на завантаження і 1,25 Гбіт/с на віддачу.

- XGS-PON

Підтримує швидкість 10 Гбіт/с як на завантаження, так і на віддачу, також використовує пасивні сплітери.

- PtMP-PON (Point-to-MultiPoint)

Одна точка OLT у провайдера підключається через пасивні сплітери (без живлення) до ONU в будинках користувачів. Переваги такої схеми — відсутність активного обладнання (сплітери пасивні), простота монтажу та висока надійність. Недолік — менша пропускна здатність для кожного абонента у пікові години, оскільки всі ділять одну загальну лінію.

- AON (Active Optical Network)

Замість пасивних сплітерів використовується Ethernet-комутатор із живленням, що дозволяє більш гнучко керувати трафіком.

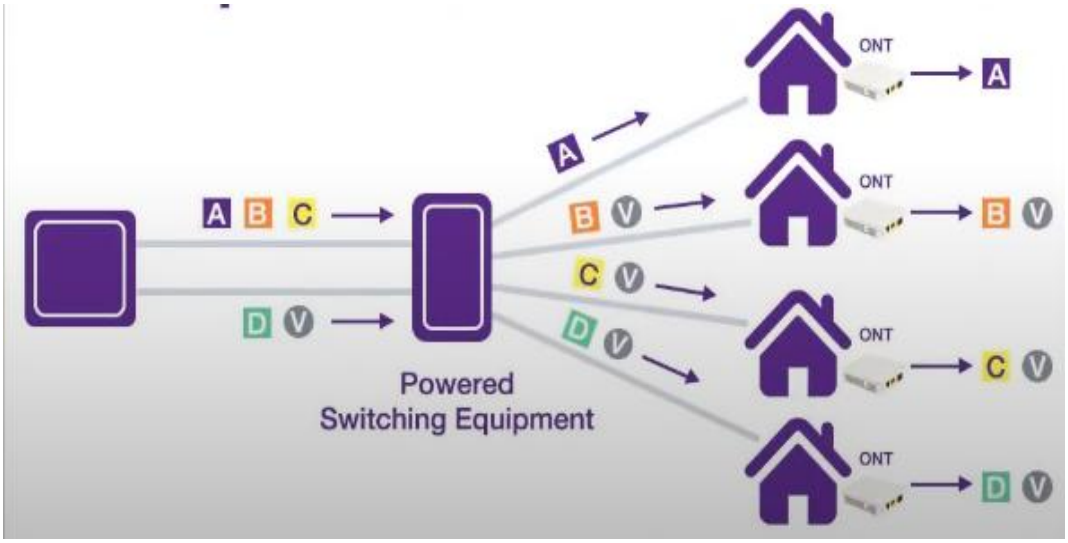

Рисунок 2.4. Схема активної волоконної мережі [33]

Переваги: більша гнучкість і можливість покривати відстані до 70 км між центральним вузлом і абонентом.

Недоліки: необхідність постійного живлення для комутатора та підвищена складність, зокрема потреба в резервній системі живлення (UPS).

Мобільний інтернет (3G/4G/4.5G/5G)

- 3G (UMTS/HSPA) дає швидкість від 0,5 до 14,4 Мбіт/с.
- 4G LTE забезпечує від 50 до 150 Мбіт/с у базових версіях, а LTE-Advanced — до 600 Мбіт/с.
- 5G NR у реальних мережах пропонує від 200 Мбіт/с до 1 Гбіт/с (частоти sub-6 GHz); на mmWave (24–28 GHz) швидкість зростає до кількох Гбіт/с із затримкою менше 10 мс.

Мобільний інтернет ідеально підходить для підключення IoT-шлюзів, особливо тих, що переміщуються. Недоліки включають більшу затримку порівняно з оптикою та залежність швидкості від навантаження базової станції.

Wi-Fi (IEEE 802.11) та Bluetooth (IEEE 802.15.1) Bluetooth Low Energy (BLE):

- Дальність до 100 м (клас 1) або 10 м (клас 2).
- Швидкість передачі даних до 2 Мбіт/с.
- Використовується для низькошвидкісних сенсорів у розумних будинках, маячках, фітнес-трекерах.

Wi-Fi:

- Wi-Fi 4 (802.11n) забезпечує до 600 Мбіт/с.
- Wi-Fi 5 (802.11ac) — до 3,5 Гбіт/с.
- Wi-Fi 6 (802.11ax) — до 9,6 Гбіт/с.
- Дальність роботи у приміщеннях становить 20–50 м, на відкритому повітрі — до 100 м.
- Використовується для швидкого локального доступу, IP-камер, розумного будинку та IoT-хабів.

Призначення мереж широкосмугового доступу:

- Для дому/офісу перевага віддається FTTH (до 1 Гбіт/с). Якщо оптика недоступна — використовують xDSL (до 100 Мбіт/с на VDSL) або DOCSIS (до 500 Мбіт/с).
- Для сільської місцевості підходить LTE-модем (50–100 Мбіт/с) або супутниковий інтернет (LEO — до 200 Мбіт/с).
- Для IoT та невеликої кількості сенсорів використовують LPWAN (LoRaWAN, NB-IoT) або BLE (при дальності до 100 м і низькій швидкості).

2.2. Архітектури проводових мереж доступу

2.2.1. Загальний опис архітектури проводових мереж доступу [10]

Архітектури FTTx пояснюють, як далеко оптоволоконний кабель прокладається до кінцевого користувача.

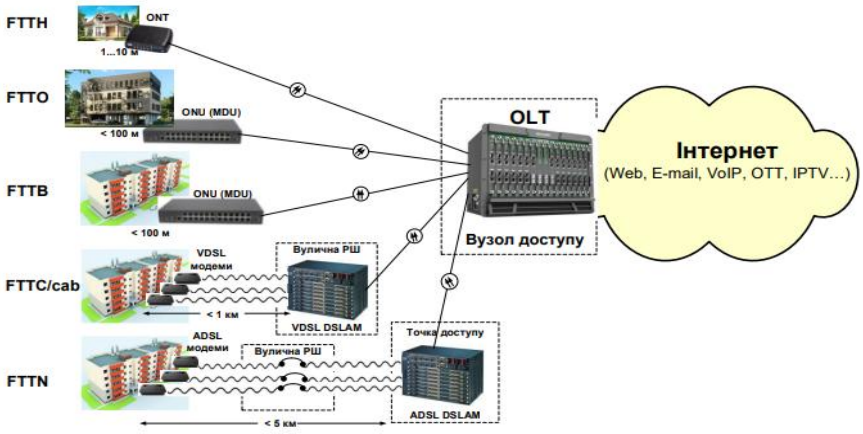

Рисунок 2.5. Архітектури мереж доступу

Основні типи архітектур проводових мереж доступу:

- **FTTH (Fiber to the Home)**: оптоволокно підводиться прямо до квартири або приватного будинку. В приміщенні встановлюють ONT (Optical Network Terminal), що перетворює світловий сигнал у електричний. Швидкість може досягати і перевищувати 1 Гбіт/с (GPON, XGS-PON). Це найякісніше і найнадійніше рішення для абонента.

- **FTTB/FTTO (Fiber to the Building / Fiber to the Office)**: волокно до технічної кімнати будинку чи офісу, далі розподіл даних мідними кабелями (витою парою чи коаксіалом) всередині. Швидкості всередині будівлі — 100–1000 Мбіт/с (Ethernet). Дешевше ніж FTTH.
- **FTTC / FTTCabinet (Fiber to the Cabinet)**: волокно до вуличної шафи, що обслуговує десятки чи сотні будинків. Від шафи до користувача — кабелі xDSL (виті пари) або DOCSIS (коаксіал). Діапазон до 500 метрів, швидкість VDSL2 — до 100 Мбіт/с на коротких відстанях.
- **FTTN (Fiber to the Node)**: волокно підводять до розподільника, що обслуговує великий район. Далі до будинків прокладається мідь. Відстань до 1–2 км, швидкість зменшується з відстанню (VDSL2 дає 50-70 Мбіт/с на 1 км).

Можливі схеми технологій FTT :

- FTTH: OLT → оптоволокно → ONT (користувач)
- FTTB/FTTO: OLT → оптоволокно до будівлі → ONU → Ethernet до квартир
- FTTC: OLT → оптоволокно до шафи → DSLAM → виті пари до користувачів
- FTTN: OLT → оптоволокно до вузла → мідь до будинків [8,10].

2.2.2. Технології приймання та відправки повідомлень

У пасивних PON (GPON, EPON) від OLT (Optical Line Terminal) до ONT одночасно обслуговується тисячі абонентів.

Для передачі двонаправленого сигналу використовують:

- **Низхідний (downstream)**: довжина хвилі 1490 нм, передача даних від OLT до ONT через часові слоти (TDM).
- **Висхідний (upstream)**: використовується довжина хвилі 1310 нм. Щоб уникнути конфліктів при одночасній передачі даних від кількох ONT, застосовується метод TDMA (множинний доступ з часовим поділом).

Контроль часових інтервалів здійснюється за протоколом MPCP (Multi-Point Control Protocol): спочатку OLT надсилає команду Gate кожному ONU,

виділяючи конкретний таймслот для передачі. Потім ONU відповідає повідомленням Report, вказуючи, скільки байтів воно готове передати. Завдяки цьому кожен ONT очікує свій час (таймслот) і передає дані без колізій

На рисунку 2.6 показано, що OLT передає пакети з інформацією про те, кому саме (якому ONT) призначений кожен таймслот. ONT приймають лише свої слоти та ігнорують інші.

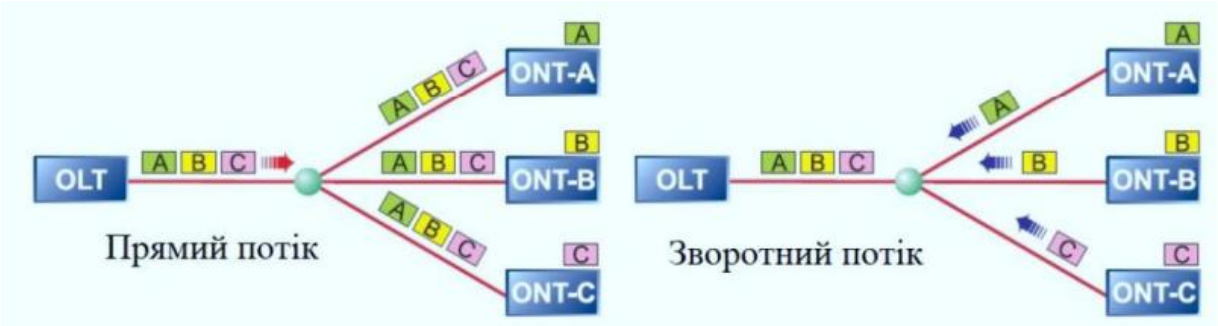

Рисунок 2.6. Мультиплексування TDM

Завдяки мультиплексуванню TDM кілька абонентів можуть одночасно використовувати один оптичний канал, розподіляючи його за часом. Це дозволяє додаватиих користувачів без необхідності прокладати окреме волокно — достатньо призначити їм новий таймслот. Такий підхід підвищує ефективність використання ресурсів і дає змогу обслуговувати велику кількість користувачів. Крім того, обладнання для TDM/TDMA є дешевшим за WDM (мультиплексування за довжиною хвилі), де потрібні складні лазери та фільтри для кожної хвилі.

Організація комутації в мережах

У будь-якій комп’ютерній мережі дані передаються не просто по кабелю, а з використанням різних методів комутації, які допомагають максимально ефективно використовувати наявну фізичну інфраструктуру.

Комутація каналів (Circuit Switching)

Перед початком передачі даних встановлюється постійний фізичний канал між відправником і отримувачем. Всі дані проходять через цей зарезервований канал без перерв.

Коли користувач А запитує з’єднання з користувачем В, маршрутизатори вибирають послідовність ліній та комутаторів, які з’єднуються в єдиний маршрут. Після встановлення з’єднання весь трафік передається по цьому шляху без додаткової маршрутизації чи буферизації. Коли передача завершується або один із учасників розриває сеанс, канал звільняється.

Переваги:

- Фіксована і відома швидкість (наприклад, 64 Кбіт/с для традиційного голосового зв’язку).
- Стабільна затримка через відсутність черг у буферах.
- Простота моделі передачі, схожа на телефонні мережі.

Недоліки:

- Резервований канал залишається пустим, якщо користувач не передає дані, що неефективно.
- Якщо всі канали зайняті, з’єднання неможливе.
- Неможливо під час сеансу динамічно змінити пропускну здатність.
- Складно об’єднувати сервіси з різними швидкостями в одному каналі (наприклад, відео 5 Мбіт/с і дані 100 Кбіт/с).

Комутація каналів вперше використала широкого застосування в телефонних мережах (PSTN), де для дзвінків виділялися окремі фізичні канали з пропускною здатністю 64 Кбіт/с на всьому маршруті від абонента А до абонента В [32].

Комутація пакетів (Packet Switching)

Великі обсяги даних розбиваються на невеликі пакети (від кількох сотень до кількох тисяч байт), кожен із яких містить заголовок із адресами відправника та отримувача. Кожен пакет пересилається незалежно, а маршрутизатори на кожному етапі вибирають найкоротший або найоптимальніший шлях.

Джерело розбиває повідомлення (наприклад, файл чи веб-сторінку) на пакети, додаючи до них IP-заголовки та іншу службову інформацію. Пакети надходять на маршрутизатор, який аналізує заголовок і визначає наступний напрямок передачі. На проміжних вузлах маршрути можуть змінюватися, що

дозволяє динамічно балансувати навантаження і обходити несправності. Отримувач збирає пакети, перевіряє їх порядкові номери і відновлює початкове повідомлення.

Переваги:

- Краще використання пропускної здатності мережі за змінного навантаження — пакети від різних користувачів спільно передаються по одному каналу.
- Гнучкість у передачі різних типів даних (відео, голос, інформація) одночасно.
- Автоматичне перенаправлення пакетів у разі виходу з ладу вузла, що зберігає стабільність з'єднання.

Недоліки:

- Затримка передачі може коливатися залежно від навантаження (джиттер).
- Пакети можуть загубитися або приходити з помилками під час пікових навантажень.
- Протоколи (наприклад, TCP/IP) складніші, вимагають буферизації, повторної передачі та контрольних сум.

Приклад:

Інтернет, включно з веб-сторінками, електронною поштою, відеоконференціями, VoIP і IPTV, використовує комутацію пакетів. Наприклад, відеопотік на YouTube розбивається на тисячі пакетів, і кожен маршрутизатор обирає для нього оптимальний шлях.

Застосування в сучасних мережах:

- Комутація каналів використовується в традиційних телефонних мережах (TDM у PSTN), де важливі гарантована швидкість і мінімальна затримка для голосового зв'язку.
- Комутація пакетів лежить в основі Інтернету та корпоративних LAN, MAN і WAN, забезпечуючи гнучкість та масштабованість для різних видів трафіку [32].

2.3. Характеристика стандартів безпроводового зв’язку для IoT.

2.3.1. Порівняння безпроводових технологій передачі даних.

Важливо не лише знати існуючі технології бездротового зв’язку, а й правильно обирати потрібну для створення мережі, яка має виконувати завдання з високою надійністю. Для цього порівнюють технології за такими критеріями:

- Дальність дії
- Енергоспоживання
- Пропускна спроможність і швидкість передачі
- Вартість

Розглянемо поділ технологій за зоною покриття (рис.2.7).

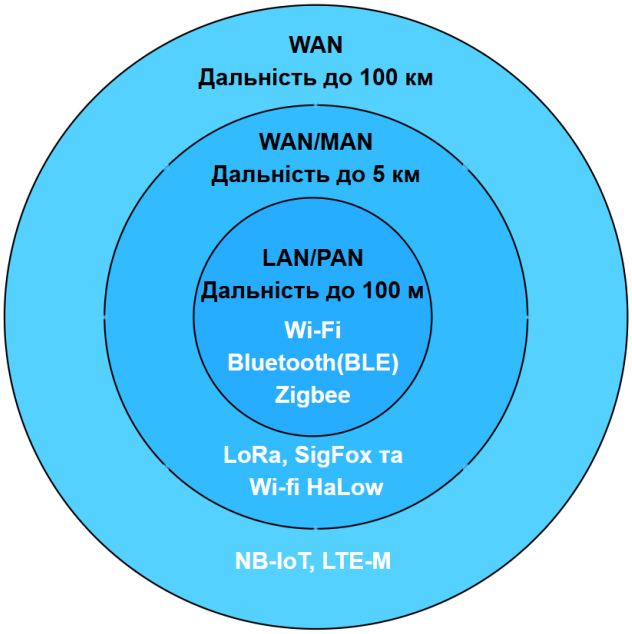

Рисунок 2.7. Розподіл безпроводових технологій за зоною покриття

- **Локальні та персональні мережі (LAN / PAN)** працюють до 100 м, застосовуються у домашньому або невеликому офісному середовищі. Технології: Wi-Fi, Bluetooth Low Energy, Zigbee. Основна мета — комунікація на коротких дистанціях, наприклад, у межах квартири чи робочого простору.
- **Міські і розширені мережі (MAN / WAN)** забезпечують покриття до 5 км. Застосовують технології LoRa, SigFox, Wi-Fi HaLow. Використовують

для розгортання смарт-інфраструктури, моніторингу довкілля, міських сенсорних мереж.

- **Глобальні мережі (WAN)** призначені для великої географічної відстані — до 50-100 км, забезпечують стабільний зв’язок між далекими точками. Технології: LTE-M, NB-IoT, які підтримують мобільні IoT-пристрої та інтеграцію з хмарою.

На рисунку 1.8 представлено порівняння технологій Інтернету речей за двома основними параметрами:

- швидкість передачі даних (Data rate);
- дальність зв’язку (Range).

Wi-Fi HaLow

Має найбільший радіус дії — до кількох кілометрів, при цьому забезпечує високу швидкість передачі: понад 80 Мбіт/с на близьких відстанях і близько 150 кбіт/с на відстані 1 км. Ця технологія добре підходить для смарт-міст і великих об’єктів.

Bluetooth Low Energy (BLE) [38]

Працює на відстані до приблизно 100 метрів зі швидкістю в кілька сотень кбіт/с. Ідеальна для переносних пристроїв і персональних мереж.

Zigbee [37]

Має дальність, подібну до BLE, але з нижчою швидкістю передачі. Широко застосовується у розумних будинках.

LoRaWAN [39]

Характеризується великою дальністю (до кількох кілометрів) і низькою швидкістю (кілька кбіт/с). Ідеальна для автономних сенсорів, особливо в сільському господарстві та інфраструктурі.

Sigfox [38]

Ще нижча швидкість передачі, але з підтримкою дуже великих дистанцій. Орієнтована на наднизьке енергоспоживання.

NB-IoT (Narrowband IoT) [38]

Працює на великих відстанях (до кількох кілометрів) зі середньою швидкістю передачі і підтримує мобільний зв’язок.

Wi-SUN

Має широкий діапазон дії і помірну швидкість передачі. Часто використовується в розподілених системах управління, наприклад, в енергетичних мережах.

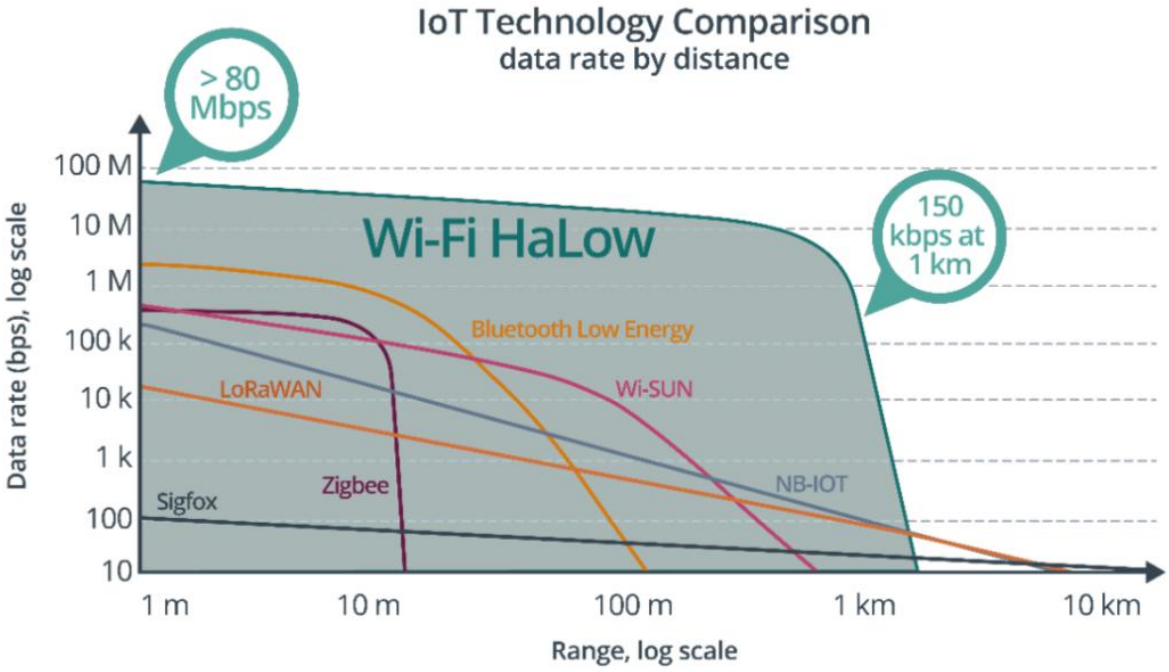

Рисунок 2.8. Порівняння технологій передачі даних в мережах IoT за швидкістю передачі даних відносно відстані.

Графік на рис.2.8 демонструє, що жодна з технологій не є універсальною — вибір залежить від конкретних потреб: чи важливіша велика швидкість, чи дальність зв’язку, чи мінімальне енергоспоживання. Wi-Fi HaLow виділяється як оптимальний компроміс між швидкістю і дальністю.

Далі можна порівняти всі основні характеристики цих технологій більш детально в табл.2.1.

Таблиця 2.1. Порівняння безпроводових технологій передачі даних в IoT-мережах

Технологія	Радіус дії	Швидкість передачі	Енергоспоживання	Частота роботи	Переваги	Недоліки
Wi-Fi	До 100 м	До 600 Мбіт/с	Високе	2.4 ГГц / 5 ГГц	Висока швидкість, широка підтримка	Високе енергоспоживання, малий радіус дії
Wi-Fi HaLow	До 1 км	Від 150 Кбіт/с до 80 Мбіт/с	Низьке	900 МГц (Sub-1 GHz)	Великий радіус, сумісність з Wi-Fi	Ще обмежена поширеність
Bluetooth	До 10 м	До 3 Мбіт/с	Середнє	2.4 ГГц	Простота, низька вартість	Короткий радіус дії
Bluetooth Low Energy (BLE)	До 50–100 м	До 2 Мбіт/с	Дуже низьке	2.4 ГГц	Дуже енергоефективний	Обмежена швидкість і радіус
ZigBee	До 100 м (до 1 км з ретрансляцією)	До 250 Кбіт/с	Низьке	2.4 ГГц / 868 / 915 МГц	Сітчаста топологія, низьке споживання	Низька швидкість, перешкоди на 2.4 ГГц
Технологія	Радіус дії	Швидкість передачі	Енергоспоживання	Частота роботи	Велика дальність, довга автономність	Дуже низька швидкість, затримка
LoRa / LoRaWAN	До 15 км	До 50 Кбіт/с	Дуже низьке	433 / 868 / 915 МГц	Мінімальне енергоспоживання, низька вартість	Обмежена кількість передач, односторонній зв’язок
Sigfox	До 10 км (місто), до 50 км (село)	До 100–600 біт/с	Дуже низьке	868 / 915 МГц	Підтримка мобільності, голосу	Вища вартість модулів, залежить від покриття LTE
LTE-M (Cat-M1)	До 10–15 км	До 1 Мбіт/с	Низьке	700–900 МГц (LTE)	Глибоке покриття, енергоощадність	Висока затримка, не підтримує голос
NB-IoT	До 15 км	До 250 Кбіт/с	Дуже низьке	700–900 МГц (LTE)	Висока швидкість, широка підтримка	Високе енергоспоживання, малий радіус дії

Аналіз таблиці показує, що розглянуті технології можна класифікувати не лише за дальністю зв’язку та швидкістю передачі даних, але й за рівнем енергоспоживання, який безпосередньо впливає на швидкість передачі.

Технології з низьким енергоспоживанням (LoRa, NB-IoT, BLE, Sigfox) підходять для тривалого роботи на батареї, однак мають обмежену швидкість передачі даних.

Натомість технології з високою швидкістю передачі (Wi-Fi, Wi-Fi HaLow, LTE-M) вимагають більшого енергоспоживання та складнішої мережевої інфраструктури.

Отже, дані Таблиці 2.1 підтверджують, що кожна технологія має свої переваги і недоліки, тому вибір конкретного рішення залежить від потреб мережі: необхідної дальності, швидкості, рівня енергоспоживання, вартості, підтримки мобільності та існуючої інфраструктури.

2.3.2. Аналіз характеристик безпроводових технологій передачі даних у мережах IoT

Під час створення IoT-мереж велике значення мають не лише самі пристрої, а й технології передачі даних. Вони визначають дальність сигналу, швидкість обміну інформацією та енергоефективність системи. Через це вибір комунікаційного протоколу є одним із найважливіших рішень при розробці Інтернету речей.

Підбір технології для IoT-систем потребує індивідуального підходу, оскільки кожен сценарій має свої особливі вимоги. Наприклад, у промислових IoT, де першочергові надійність і низька затримка, оптимальним вибором стануть 5G або Ethernet. Натомість для розумних міст або сільського господарства, де важлива енергоефективність і широке покриття, кращими будуть протоколи на кшталт LoRaWAN чи NB-IoT.

Вибір протоколу передачі даних є ключовим фактором, що впливає на ефективність роботи мережі IoT. Саме від нього залежить стабільність зв’язку, тривалість автономної роботи пристроїв та загальна здатність системи виконувати свої завдання.

Далі наведено огляд основних безпроводових технологій передачі даних, які найчастіше застосовуються в IoT, та їхніх ключових особливостей.

Wi-Fi [36]

Wi-Fi (Wireless Fidelity) — одна з найпопулярніших і найпоширеніших бездротових технологій, заснована на стандартах IEEE 802.11. Вона дозволяє передавати дані через радіоканали в діапазонах 2,4 ГГц, 5 ГГц, а у новіших версіях — також 6 ГГц.

Wi-Fi широко застосовується в системах розумного дому, офісної автоматизації, а також у медичних та безпекових рішеннях. Наприклад, більшість сучасних розумних телевізорів, камер відеоспостереження, голосових асистентів (Google Home, Alexa) і термостатів підключаються саме через Wi-Fi.

Однією з головних переваг Wi-Fi є висока швидкість передачі даних — понад 1 Гбіт/с у стандартах Wi-Fi 5 і Wi-Fi 6. Це дозволяє ефективно передавати аудіо- та відеопотоки в режимі реального часу, обробляти великі обсяги інформації й підтримувати інтерактивні функції. Окрім того, Wi-Fi має широку інфраструктурну підтримку, що полегшує інтеграцію, оскільки мережі Wi-Fi є у більшості будинків і офісів.

Втім, у Wi-Fi є обмеження по радіусу дії. У приміщеннях сигнал зазвичай стабільний на відстані 50–100 метрів, проте на якість сигналу впливають перешкоди, такі як стіни. Частота 2,4 ГГц є загальною для багатьох пристроїв, що може призводити до перевантаження мережі і збоїв у з’єднанні. Для забезпечення стабільного зв’язку у великих приміщеннях потрібні додаткові точки доступу або ретранслятори.

Таким чином, Wi-Fi є ефективним вибором для IoT-систем із постійним живленням, які потребують високошвидкісного обміну даними. Однак для застосувань, де важлива автономність і низьке енергоспоживання, доцільно розглядати інші бездротові технології.

Wi-Fi HaLow [40]

Wi-Fi HaLow — це спеціалізована версія Wi-Fi, розроблена для пристроїв Інтернету речей, яка базується на стандарті IEEE 802.11ah. На відміну від

звичайного Wi-Fi, HaLow працює у частотній смузі нижче 1 ГГц (переважно в діапазоні 750–950 МГц).

Такий діапазон забезпечує більший радіус дії — до 1 км на відкритому просторі, кращу проникність сигналу через стіни та інші перешкоди. Крім того, Wi-Fi HaLow характеризується нижчим енергоспоживанням, що робить технологію оптимальною для масштабних та енергоефективних IoT-систем.

Максимальна швидкість передачі даних у Wi-Fi HaLow варіюється від 150 Кбіт/с до 78 Мбіт/с, залежно від умов і налаштувань мережі.

Важливою особливістю є підтримка одночасного підключення тисяч пристроїв до одного маршрутизатора, що робить Wi-Fi HaLow привабливим для промислових об’єктів, великих комплексів і розумних міст.

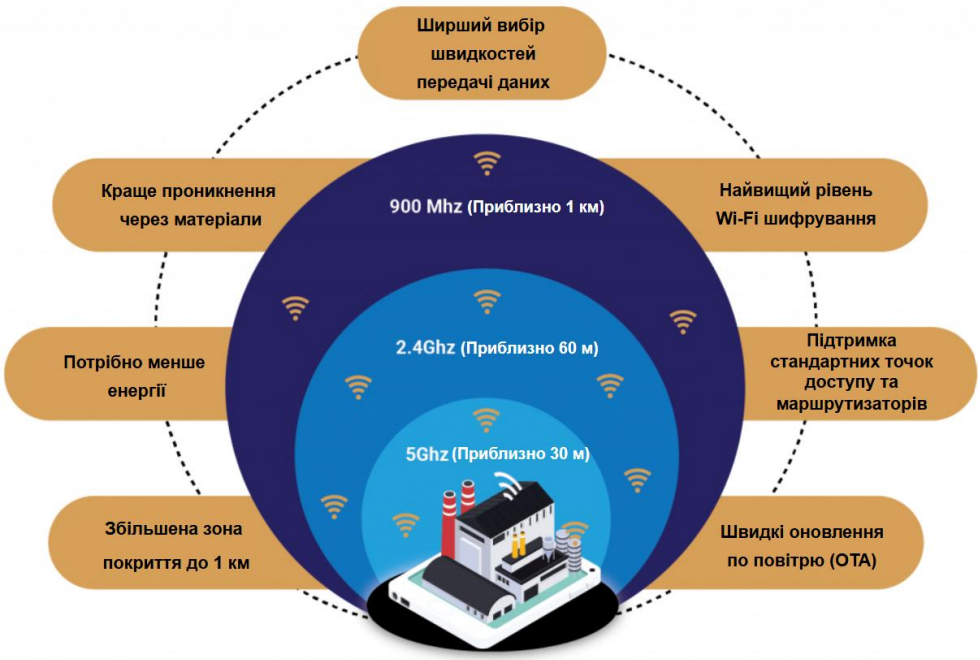

Рисунок 2.9. Переваги технології Wi-Fi HaLow впорівнянні з звичайним Wi-Fi. [41]

Нижча швидкість передачі даних у Wi-Fi HaLow порівняно з Wi-Fi 5 або Wi-Fi 6 робить цю технологію менш придатною для потокового відео, мультимедіа або обробки великих обсягів даних у режимі реального часу.

Водночас Wi-Fi HaLow є перспективним рішенням для IoT-систем, оскільки поєднує переваги широкого покриття, низького енергоспоживання та підтримки IP-з’єднань. Ця технологія набирає популярність у промисловому Інтернеті речей, розумних містах, агротехнологіях та інших масштабних застосуваннях.

Bluetooth Low Energy (BLE) [42]

Bluetooth Low Energy — це енергоефективна бездротова технологія зв’язку, яка є складовою стандарту Bluetooth 4.0 і вище. Вона розроблена для застосувань з мінімальним енергоспоживанням, а не для високошвидкісної передачі даних.

BLE дозволяє пристроям обмінюватися невеликими обсягами інформації на коротких відстанях, що робить її ідеальним рішенням для Інтернету речей, особливо у випадках, де важлива тривала автономна робота пристроїв на батареях.

Технологія широко використовується у переносних пристроях, таких як фітнес-браслети, розумні годинники, медичні сенсори, маячки (beacons), системи моніторингу навколишнього середовища, а також у рішеннях для розумного дому, де потрібно забезпечити періодичний або постійний зв’язок між сенсором і центральним пристроєм (наприклад, смартфоном чи шлюзом).

Технічні характеристики BLE:

- Працює в частотному діапазоні 2.4 ГГц, як і класичний Bluetooth.
- Радіус дії може досягати до 100 метрів на відкритому просторі, проте в закритих приміщеннях ця відстань зазвичай менша.
- Максимальна швидкість передачі даних — до 1 Мбіт/с, а у версії BLE 5.0 – до 2 Мбіт/с, що достатньо для передачі коротких повідомлень і сенсорних даних.
- Підтримує mesh-мережі, що дозволяють об'єднувати велику кількість пристроїв у взаємодіючі мережі, розширюючи зону покриття і підвищуючи надійність передачі навіть у складних умовах.

Zigbee [37]

Zigbee — це низькопотужна бездротова технологія зв’язку, створена для передачі невеликих обсягів даних між пристроями в мережах Інтернету речей. Вона базується на стандарті IEEE 802.15.4 і працює у діапазонах 2,4 ГГц, а також 868 МГц і 915 МГц у певних регіонах.

Zigbee широко застосовується в розумних будинках, системах автоматизації, сенсорних мережах, освітленні, моніторингу навколишнього середовища та інших IoT-застосуваннях, де важливі низьке енергоспоживання, надійність і легкість інтеграції.

Технічні особливості Zigbee:

- Працює в безліцензійних діапазонах, зазвичай 2,4 ГГц.
- Радіус дії варіюється від 10 до 100 метрів залежно від умов навколишнього середовища та потужності передавача.
- Швидкість передачі досить низька — до 250 Кбіт/с, що цілком підходить для обміну простими датчиками та актуаторами, наприклад, станом дверей, температурою чи рівнем освітлення.

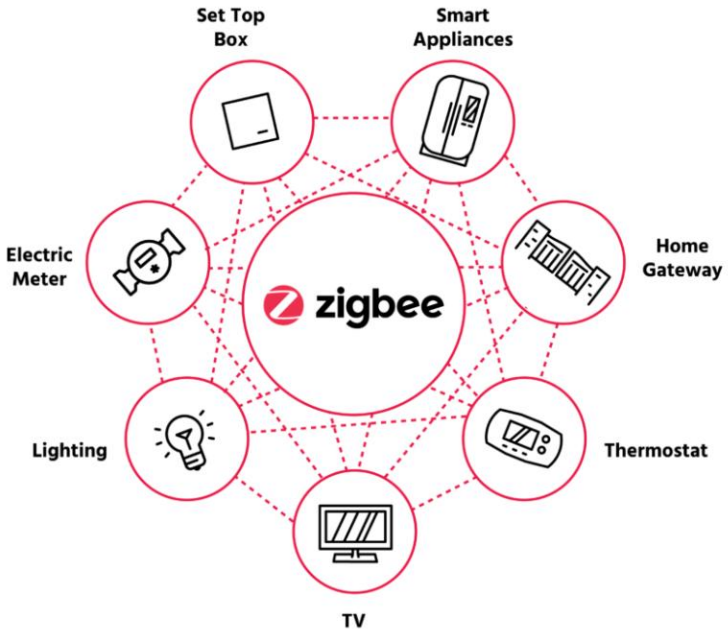

Рисунок 2.10. – Вигляд IoT-мережі, яка використовує технологію Zigbee.

Однією з важливих особливостей Zigbee є підтримка mesh-мережі — сіткоподібної структури, в якій кожен пристрій може передавати дані іншим. Така архітектура підвищує надійність зв’язку, допомагає обходити перешкоди

та розширює загальний радіус дії мережі без необхідності використання потужних передавачів.

Водночас варто враховувати, що Zigbee працює у частотному діапазоні 2.4 ГГц, де зіштовхується з конкуренцією від Wi-Fi, Bluetooth та інших пристроїв, що може спричиняти зниження якості сигналу через перешкоди.

LoRa

LoRa (Long Range) — енергоефективна бездротова технологія, розроблена для передачі невеликих обсягів даних на великі відстані. Вона належить до класу LPWAN (Low Power Wide Area Network), що забезпечує низьке енергоспоживання і широке покриття. Це робить LoRa ідеальною для IoT-рішень у розподілених системах, наприклад у сільському господарстві, моніторингу навколишнього середовища, розумних містах та інфраструктурі.

LoRa працює у неліцензованих частотних діапазонах — 433 МГц, 868 МГц (Європа) і 915 МГц (Америка), що дозволяє уникнути плати за радіочастоти.

- Дальність дії: до 15 км у сільській місцевості, 2–5 км у містах.
- Швидкість передачі: від 0,3 до 50 Кбіт/с.
- Енергоспоживання: дуже низьке, пристрої можуть працювати на батареї до 5–10 років.

Переваги LoRa:

- Висока дальність покриття без потреби у великій інфраструктурі.
- Низьке енергоспоживання для тривалого терміну роботи пристроїв.
- Підтримка великої кількості пристроїв на одній базовій станції.
- Можливість створення приватних мереж без залежності від мобільних операторів.
- Надійність та безпека завдяки наскрізному шифруванню даних (AES-128).

Sigfox [39]

Sigfox — це спеціалізована LPWAN-технологія для підключення IoT-пристроїв із мінімальним енергоспоживанням, яка орієнтована на передачу

невеликих обсягів даних. Вона функціонує в неліцензованих радіочастотах: 868 МГц у Європі, 902 МГц у США та 433 МГц у деяких азійських країнах.

На відміну від Wi-Fi або мобільного зв'язку, Sigfox не забезпечує широкосмуговий доступ, а оптимізована для передачі коротких повідомлень з мінімальною частотою, кілька разів на день.

Енергоспоживання дуже низьке, пристрої можуть працювати до 10 років на одній батареї.

Дальність зв'язку: 40–50 км у відкритій місцевості, 10–15 км у місті.

Однак Sigfox має обмеження:

- Передача невеликих пакетів (до 12 байтів на повідомлення).
- Обмеження на кількість вихідних повідомлень — до 140 на день.
- Обмежена кількість вхідних повідомлень (downlink) — до 4 на день.
- Залежність від доступності базових станцій Sigfox, які користувач не може самостійно розгорнути.
- Не підходить для задач у режимі реального часу через затримки і обмежену частоту передачі.

NB-IoT (Narrowband Internet of Things)

NB-IoT — це радіотехнологія з вузькою смугою пропускання, що відноситься до класу LPWAN і створена для ефективного, енергоощадного та стабільного зв'язку між IoT-пристроями у межах стільникових мереж. Розробку NB-IoT ініціювали провідні телекомунікаційні компанії (Huawei, Ericsson, Nokia) за участю організації 3GPP, яка займається стандартизацією мобільного зв'язку (4G, 5G).

Технологія призначена для масового підключення пристроїв, які надсилають невеликі обсяги даних та працюють у складних умовах, таких як підвали, шахти або промислові зони.

Технічні характеристики NB-IoT:

Працює у ліцензованих діапазонах частот, використовуючи існуючу інфраструктуру стільникових операторів.

Три режими роботи:

- у межах LTE-мережі (in-band);

- у охоронній смузі між LTE-каналами (guard band);
- автономно (standalone), наприклад, на частотах GSM.
- Максимальна швидкість передачі — до 250 Кбіт/с (як у завантаженні, так і у віддачі).
- Дальність зв’язку — до 10–15 км у сільській місцевості, 2–5 км у місті.
- Підтримка великої кількості пристроїв — до 50 000 на одну базову станцію.
- Глибоке покриття, що дозволяє працювати навіть у тунелях, підземних паркінгах і за товстими бетонними стінами.

Обмеження:

- Затримки передачі можуть бути завеликі для застосувань, що потребують миттєвої реакції.
- Відсутність підтримки голосового зв’язку та мобільності (неможливість хендоверів), що робить технологію непридатною для рухомих об’єктів.

LTE-M (LTE Cat-M1)

LTE-M — це стандарт мобільного зв’язку, створений 3GPP спеціально для Інтернету речей. Він також відноситься до технологій LPWAN і працює в межах існуючої LTE-мережі, що робить його широко доступним без потреби будувати нову інфраструктуру.

LTE-M орієнтований на пристрої з низьким енергоспоживанням, помірною швидкістю передачі і тривалим терміном автономної роботи. На відміну від NB-IoT, LTE-M підтримує мобільність і передачу голосу через VoLTE.

Основні характеристики:

- Використовує смугу частот шириною 1,4 МГц.
- Максимальна швидкість передачі — до 1 Мбіт/с у обох напрямках.
- Низька затримка (50–100 мс), що дозволяє застосовувати LTE-M у реальному часі.

- Забезпечує широке покриття з підтримкою роумінгу, що особливо важливо для міжнародних IoT-рішень.

2.4. Комплексна безпека IoT в мережевих технологіях

Забезпечення надійності передачі інформації є одним із ключових пріоритетів при організації мережевого забезпечення роботи IoT [43]. Аналіз основних загроз безпеці у технологіях IoT дозволяє зробити такі висновки.

Обмежена пам’ять вбудованих пристроїв ускладнює впровадження криптографічних засобів захисту через можливість переповнення буферів і обмеження на зберігання ключів.

Переповнення буферів створює ризик впровадження шкідливого коду або його виконання у вразливих ділянках пам’яті. Це призводить до появи системних вразливостей, які можуть бути використані зловмисниками для компрометації системи, несанкціонованого виконання коду або витоку конфіденційних даних.

Через **обмежену пам’ять для зберігання криптографічних ключів** виникає ризик їх компрометації. Управління ключами, що є критичною складовою безпеки даних, ускладнюється через обмеження пам’яті, що може призвести до використання ненадійних або повторно використовуваних ключів.

Ефективне зберігання, оновлення та ротація ключів вимагає ресурсів, які обмежені у вбудованих пристроях. Неправильне управління збільшує доступність ключів для атакуючих та підвищує ймовірність успішних атак, спрямованих на отримання ключів. Отже, криптографічний захист стає вразливим через технічні обмеження пристроїв — переповнення буферів і складнощі із зберіганням ключів.

Незадовільне енергоспоживання в автономних IoT-модулях може перешкоджати роботі криптографічних механізмів як через конструктивні обмеження, так і унаслідок навмисного впливу на енергетичні компоненти.

Атаки, спрямовані на збільшення енергоспоживання пристроїв шляхом постійної активації, можуть призвести до швидкого розряду батарей, відключення або порушення роботи пристрою. Особливо це критично для пристроїв, що живляться від батарей або в умовах обмеженого живлення. Надмірне споживання знижує продуктивність і ефективність пристрою, роблячи його більш вразливим до атак і обмежуючи функціонування захисних механізмів.

Режими енергозбереження, спрямовані на економію ресурсу, можуть викликати затримки у виявленні атак або аномалій, оскільки пристрій у режимі очікування менш активний, що зменшує його чутливість до змін у навколишньому середовищі. У таких випадках критично важливі швидкі реакції на загрози, і затримки можуть призводити до негативних наслідків.

Обмежене енергоспоживання ускладнює своєчасне виявлення і реагування на загрози, що підвищує ризики безпеки та знижує загальну надійність системи.

Криптографічні алгоритми зазвичай є ресурсомісткими, тому недостатня обчислювальна потужність пристроїв має декілька негативних наслідків:

Несумісність ресурсів пристрою з вимогами складних алгоритмів шифрування може змушувати використовувати менш надійні методи, що робить систему більш вразливою.

Обмеження обчислювальних ресурсів може обмежувати можливості впровадження надійної автентифікації, включно з біометричними способами, підвищуючи вразливість до атак. Також ускладнюється зберігання і управління паролями, ключами і іншою ідентифікаційною інформацією.

У режимах низького енергоспоживання часто застосовуються спрощені алгоритми шифрування, що знижує рівень захисту даних і робить їх більш вразливими.

Компроміс між економією енергії та ефективністю шифрування позначається на безпеці, підвищуючи ймовірність атак. Особливо це ускладнює відновлення захищеної інформації після інцидентів безпеки або несанкціонованого доступу.

Відновлення нормальної роботи пристрою після відключення живлення може бути складним через втрату інформації про попередній стан і поточні дані, що безпосередньо впливає на надійність і працездатність IoT-систем.

Висновки до розділу 2

У другому розділі розглянуто перспективи розвитку мережних технологій в Інтернеті речей. Проведено аналіз тенденцій розвитку та інновацій, що відображають стрімке зростання світового ринку і впровадження як проводових, так і бездротових технологій (зокрема 5G, Wi-Fi 6, LPWAN), а також хмарних і безпекових рішень.

Розглянуто основні проблеми інтеграції мережевих технологій з іншими компонентами IoT та запропоновано методи їх вирішення, серед яких використання сучасних алгоритмів шифрування, створення ізольованих сегментів мережі та впровадження багаторівневої аутентифікації.

Проведене порівняння технологій за ключовими параметрами — максимальною дальністю роботи, енергоспоживанням і швидкістю передачі даних — дозволило визначити оптимальні сфери їх застосування. Таким чином, вибір відповідної технології є одним із найважливіших кроків для створення надійних та ефективних IoT-мереж.

Проаналізовано призначення основних компонентів мережі та питання оптимізації її архітектури. Показано, що для досягнення високого рівня доступності потрібен комплексний підхід, який включає технічні рішення, стратегічне планування і постійний моніторинг мережі.

3. АНАЛІЗ НАПРЯМКІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ

3.1. Аналіз відповідності стандартів мережевого зв’язку умовам реалізації застосунків IoT

Розгляд протоколів взаємодії мереж IoT в напрямку підвищення їх ефективності

За ініціативою кількох міжнародних організацій, серед яких ISO та ITU-T, було розроблено модель, що суттєво вплинула на розвиток телекомунікаційних і комп’ютерних мереж. Ця модель відома як модель взаємодії відкритих систем (Open System Interconnection, OSI), або просто модель OSI. Вона систематизує процес взаємодії між системами, встановлюючи стандартні назви рівнів та визначаючи функції кожного з них. Розробка базувалась на досвіді створення глобальних комп’ютерних мереж у 1970-х роках і описана у детальному документі обсягом понад тисячу сторінок.

Модель OSI поділяє систему комунікації на сім рівнів: прикладний, представницький, сеансовий, транспортний, мережевий, канальний та фізичний. Кожен рівень відповідає за окремі аспекти взаємодії між мережевими пристроями [44].

Модель описує компоненти взаємодії, що реалізуються через операційні системи, утиліти або апаратні засоби, але не охоплює безпосередню взаємодію користувацьких програм. Оскільки прикладний рівень OSI забезпечує системні ресурси для організації зв’язку, важливо відокремлювати його від взаємодії між самими користувацькими застосунками.

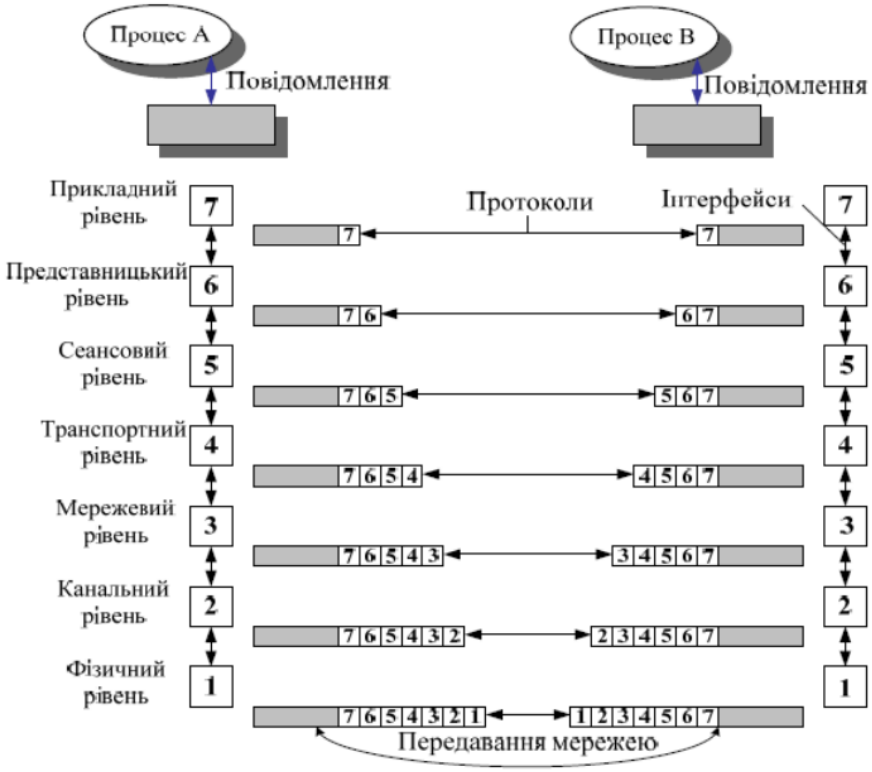

Рисунок 3.1 - Модель взаємодії систем OSI [31]

– Протокольна модель мережевої взаємодії TCP/IP

Стек TCP/IP був розроблений за ініціативою Міністерства оборони США (Department of Defense, DoD) з метою інтеграції експериментальної мережі ARPAnet з іншими мережами. Цей універсальний набір протоколів створювався для забезпечення взаємодії у різнорідних обчислювальних середовищах [45].

Великий внесок у розвиток TCP/IP зробив Університет Берклі, впровадивши ці протоколи у свою версію операційної системи UNIX. Популярність UNIX сприяла широкому розповсюдженню протоколів TCP, IP і інших, що входять до складу TCP/IP. Нині цей стек є основою взаємодії комп'ютерів в Інтернеті і широко застосовується в корпоративних мережах [46].

–

Рівні моделі TCP/IP	Призначення рівня моделі TCP/IP
4. Рівень додатків	Представлення даних користувачу, кодування і управління діалоговими вікнами.
3. Транспортний рівень	Підтримка зв'язку між різними пристроями в різних мережах.
2. Міжмережевий рівень	Визначення оптимального шляху через мережу.
1. Рівень мережевого доступу	Управління пристроями і середовищами, що формують мережу.

Рисунок 3.2 - Рівні стеку та їх призначення

3.1.2. Розгляд протоколів TCP/IP для ефективної підтримки технологій IoT за рівнями моделі OSI

Сімейство протоколів TCP/IP можна розглядати у контексті еталонної моделі OSI. У моделі OSI рівень доступу до мережі і рівень застосувань у TCP/IP розділяються для більш детального визначення функцій, які виконуються на кожному з цих рівнів [47].

Рівні моделі OSI	Основні протоколи	Рівні моделі TCP/IP
Рівень додатків Рівень представлення Сеансовий рівень	HTTP, DNS, DHCP, FTP	Рівень додатків
Транспотрний рівень	TCP, UDP	Транспотрний рівень
Мережевий рівень	IPv4, IPv6, ICMPv4, ICMPv6	Міжмережевий рівень
Канальний рівень Фізичний рівень	PPP, Frame Relay, Ethernet	Рівень мережевого доступу

Рисунок 3.3 - Порівняння моделей OSI та TSP/IP[33]

На рівні доступу до мережі протокол TCP/IP не визначає конкретний набір протоколів. Замість цього, він регламентує процедуру передачі пакетів між міжмережевим рівнем і рівнем мережевого доступу, використовуючи стандарти, які відповідають першому та другому рівням моделі OSI і регулюються іншими організаціями зі стандартизації.

Повне відповідність між моделями TCP/IP і OSI відзначається на 3-му і 4-му рівнях OSI. Мережевий рівень (рівень 3) відповідає за процеси

маршрутизації та адресації повідомлень у мережах передачі даних. Протокол IP, що входить до стеку TCP/IP, забезпечує функціональність цього рівня.[48]

Транспортний рівень (рівень 4 OSI) охоплює сервіси і функції, необхідні для впорядкованої та надійної доставки даних між вузлами. Це включає підтвердження отримання, корекцію помилок і відновлення правильного порядку пакетів. Основними протоколами на цьому рівні TCP/IP є TCP і UDP.

Прикладний рівень TCP/IP охоплює кілька протоколів, які забезпечують різноманітні функції для програм кінцевих користувачів. У моделі OSI рівні 5 (сеансовий), 6 (представницький) та 7 (прикладний) слугують орієнтирами для розробників і постачальників програмного забезпечення, що використовується у мережевих додатках.

Хоча формально модель TCP/IP має чотири рівні, багато експертів розглядають її як 5-рівневу структуру, де два нижні рівні моделі OSI (фізичний і канальний) об’єднуються в один рівень доступу до мережі [48].

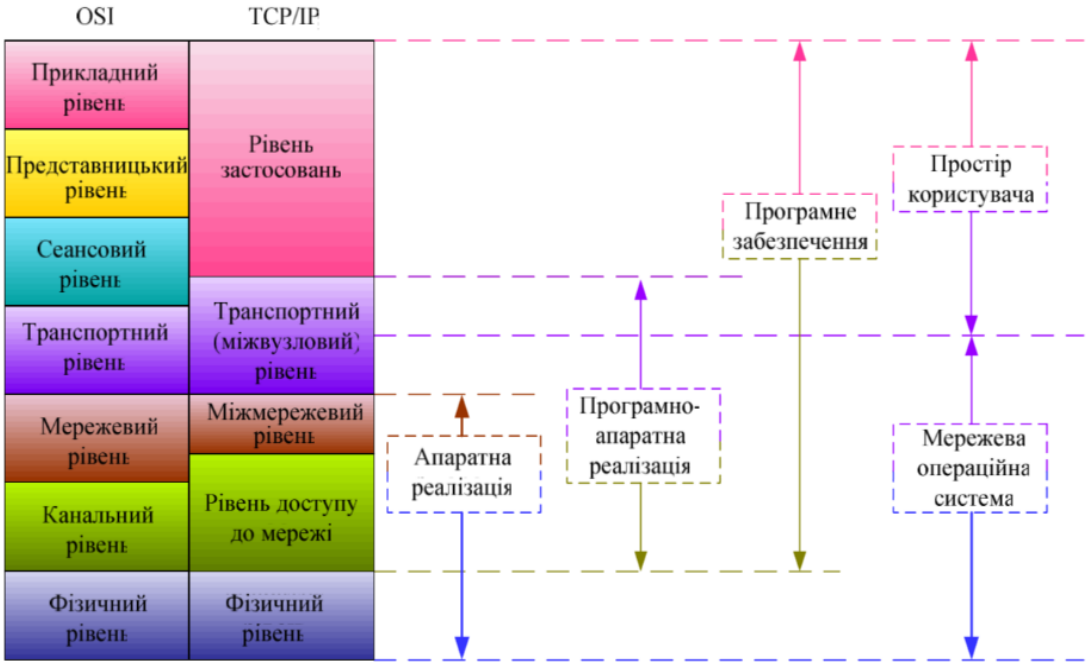

Рисунок 3.4 - Порівняння архітектур зв'язку TCP/IP і OSI та засоби реалізації різних рівнів[35]

Розглядаючи порівняння двох архітектур зв’язку — TCP/IP і OSI, можна виділити необхідні технології та протоколи для організації зв’язку між кінцевими пристроями і шлюзами, а також між шлюзом і сервером [48].

Основний протокол: IP (Internet Protocol)

IPv4

Містить 32-бітні IP-адреси (наприклад, 192.168.0.10). Підтримує субнети та NAT, що дозволяє приватним мережам взаємодіяти з Інтернетом. Більшість IoT-пристроїв у корпоративних мережах досі використовують IPv4.[49]

IPv6

Використовує 128-бітні адреси (наприклад, 2001:db8::1), що забезпечує практично необмежену кількість унікальних адрес. Це особливо важливо для сотень мільйонів IoT-датчиків. IPv6 має вбудовані механізми автоконфігурації (SLAAC) і спрощену обробку заголовків, що покращує ефективність мережі.[50]

Фізичний рівень

Цей рівень включає пристрої, протоколи та середовище передачі даних (дроти, радіочастоти тощо), які були детально описані у розділі 2.

BLE (Bluetooth Low Energy)

Технологія з низьким енергоспоживанням, що забезпечує покриття до 100 метрів в ідеальних умовах, зазвичай 10–30 метрів, зі швидкістю до 1 Мбіт/с. Вона широко застосовується у «розумних» гаджетах для тривалої роботи від батарей.[42]

ZigBee (IEEE 802.15.4)

Працює на частотах 2,4 ГГц, 868 МГц (Європа) та 915 МГц (США) зі швидкістю до 250 Кбіт/с і дальністю до 100 метрів у відкритому просторі. Призначений для побудови енергоефективних мереж типу «розумний дім» та промислової автоматизації [37].

LoRaWAN (LPWAN)

Працює в незахищеному ISM-діапазоні (868 МГц у Європі, 915 МГц у США) зі швидкістю від 0,3 до 50 Кбіт/с залежно від модуляції. Забезпечує покриття до 15 км у відкритій місцевості і 2–5 км у міських умовах. Використовується для сенсорів у сільському господарстві, міського моніторингу і «розумних» лічильників [44].

Wi-Fi (IEEE 802.11)

Працює в діапазонах 2,4 ГГц та 5 ГГц, у стандарті Wi-Fi 6 (802.11ax) забезпечує швидкість до 9,6 Гбіт/с. Радіус дії до 50 метрів у приміщеннях і до 100 метрів на відкритому повітрі. Підходить для відеокамер, систем розумного будинку, де енергоспоживання не є критичним фактором [39].

Рівень доступу до мережі

Цей рівень відповідає за обмін кадрами між пристроями, виявлення та виправлення помилок. У IoT найчастіше використовуються такі стандарти:

IEEE 802.15.4

Основний стандарт для низькоенергетичних мереж. Будь-які «зіркоподібні» чи «сіткові» мережі типу ZigBee, Thread, 6LoWPAN базуються на 802.15.4. Швидкість передачі — до 250 Кбіт/с, діапазон — до 100 м. Канальний рівень виконує контроль доступу (CSMA/CA) та перевірку CRC у кадрах.[51]

LoRa MAC (частина LoRaWAN)

Розташований над фізичним шаром LoRa. Визначає правила передачі даних вузлами на базову станцію, підтримує адаптивну швидкість передачі (ADR) для збереження енергії.[40]

Wi-Fi (IEEE 802.11)

MAC-рівень з контролем доступу CSMA/CA, шифруванням WPA2/WPA3 та перевіркою кадрів. Цей протокол є більш «важким» і підходить для пристроїв із постійним живленням.

Ethernet (IEEE 802.3)

MAC із CSMA/CD (виявлення зіткнень), фізичною адресацією (MAC-адреси). Забезпечує передачу кадрів на швидкостях від сотень Мбіт/с до десятків Гбіт/с.

Bluetooth Classic та BLE

MAC-рівень із часовим поділом каналу (TDMA) і контролем помилок. У BLE MAC оптимізований для коротких пакетів і низького енергоспоживання, забезпечуючи час відгуку в межах кількох мілісекунд [42].

Міжмережевий рівень

Міжмережевий рівень відповідає за передачу даних між хостами, здійснюючи маршрутизацію через різні вузли однієї або кількох логічних мереж. Цей рівень визначає, як пакети рухаються мережею, враховуючи адресацію, вибір оптимального маршруту та контроль за передачею даних.[49]

Основні функції міжмережевого рівня включають:

- Вибір найкращого маршруту для передачі даних між вузлами.
- Присвоєння унікальних IP-адрес для хостів і мережевих пристроїв.
- Фрагментація великих блоків даних на пакети і їх збір на приймальній стороні.
- Аналіз мережевих маршрутів для забезпечення ефективної передачі інформації.

У системах Інтернету речей міжмережевий рівень забезпечує обмін даними через маршрутизатори за допомогою таких протоколів, як IP і 6LoWPAN. Хоча багато IoT-протоколів досі використовують IPv4, у сучасних реалізаціях перевага віддається IPv6 — останній версії IP, яка покращує маршрутизацію трафіку, виявлення та адресацію пристроїв.

Протокол 6LoWPAN особливо підходить для пристроїв з обмеженими ресурсами та низьким енергоспоживанням і широко застосовується у IoT-середовищах [49].

Застосування міжмережевого рівня:

Використовується у глобальних і локальних мережах, де IP-протокол забезпечує передачу даних через Інтернет, адже саме цей протокол дозволяє ефективно обслуговувати велику кількість користувачів. Оптимізована маршрутизація між серверами полегшує обробку запитів у хмарних сервісах, а Підтримка безпеки в IoT реалізується за допомогою механізмів шифрування та авторизації, впроваджених на мережевому рівні [50].

Рівень застосунків

На цьому рівні працюють конкретні IoT-протоколи та сервіси, що полегшують розробку і взаємодію пристроїв. Усі пристрої Інтернету речей обмінюються повідомленнями за допомогою протоколів рівня застосунків.

Найпоширенішою архітектурою є модель «видавець → брокер → підписник» (Publisher–Subscriber, Pub/Sub), яка працює за простою схемою:

1. Видавець (Publisher) збирає дані, наприклад, від сенсора вологості.

2. Ці дані надсилаються до брокера — сервера, що приймає та розподіляє повідомлення.

3. Підписники (Subscriber), які підписалися на певну тему (topic), отримують відповідні повідомлення [31].

Протокол MQTT (Message Queuing Telemetry Transport)

MQTT — це легкий протокол з архітектурою Pub/Sub, розроблений спеціально для пристроїв з обмеженими ресурсами, такими як мала пам’ять і процесорна потужність. Він дуже популярний у системах «розумного» дому, промисловому моніторингу та аграрному секторі [9].

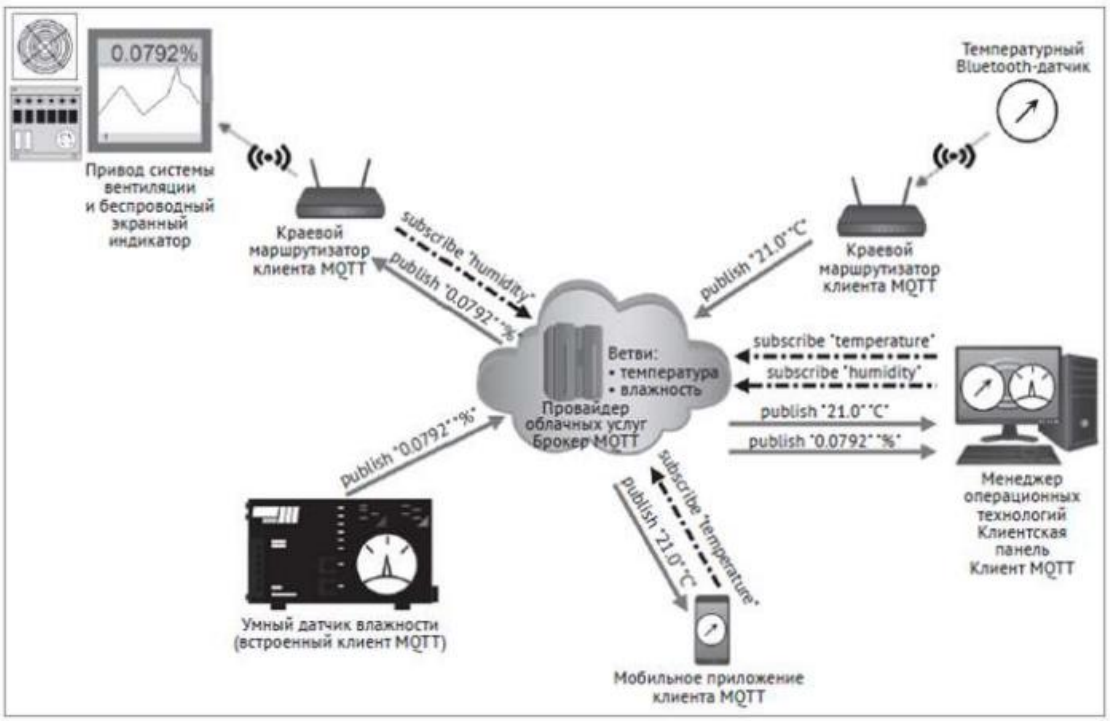

Рисунок 3.5 — Основні принципи взаємодії MQTT[8]

Основні технічні характеристики:

Працює поверх TCP, зазвичай на портах 1883 (незашифровані з’єднання) або 8883 (TLS-з’єднання).

Повідомлення підтримують три рівні якості обслуговування (QoS):

QoS 0 — «одноразова відправка» без підтвердження.

QoS 1 — гарантія доставки хоча б один раз (можливі дублікати).

QoS 2 — доставка точно один раз без дублікатів (повільніша).

Має малий розмір заголовка (усього 2 байти), що дозволяє запускати протокол на пристроях із низькими ресурсами (наприклад, Raspberry Pi або ESP32).

Існують безкоштовні хмарні брокери (CloudMQTT, HiveMQ), що дає змогу обійтися без власного сервера.

Вибір стеку протоколів у IoT залежить від кількох факторів:

- Енергоспоживання — чи пристрої живляться від батарей, чи від мережі.
- Дальність зв'язку — наприклад, BLE охоплює кілька метрів, LoRaWAN — десятки кілометрів.
- Швидкість передачі — ZigBee/6LoWPAN забезпечують до 250 Кбіт/с, LoRa — до 50 Кбіт/с.
- Потреба в надійності (TCP, DDS) або в мінімальній затримці (UDP, CoAP).

Для стабільної роботи IoT-системи критично обрати правильні протоколи на кожному рівні — від фізичного рівня до рівня застосунків. Це гарантує своєчасну доставку даних, збереження енергії пристроями та їх безпеку.

3.2. Аналіз ефективності мережевих технології для обробки IoT-трафіку та напрями її підвищення

3.2.1. Аналіз критеріїв оптимізація мережевої архітектури

Оптимізація мережевої архітектури за допомогою впровадження mesh-мереж відкриває нову парадигму в організації IoT-систем. Завдяки здатності кожного пристрою функціонувати як маршрутизатор для інших, створюється самоорганізована та самовідновлювана мережа, яка автоматично адаптується до змін топології. Це особливо важливо для географічно розподілених IoT-

систем, де традиційні централізовані структури часто бувають неефективними.[52]

Edge computing означає суттєвий перехід від централізованої до розподіленої обробки даних. Переміщення обчислювальних потужностей ближче до джерел інформації не лише знижує залежність від центральних серверів, але й дає змогу приймати критично важливі рішення в реальному часі навіть при проблемах із підключенням до хмарних сервісів. Це особливо актуально для промислових IoT-систем, де затримки можуть спричинити аварійні ситуації.

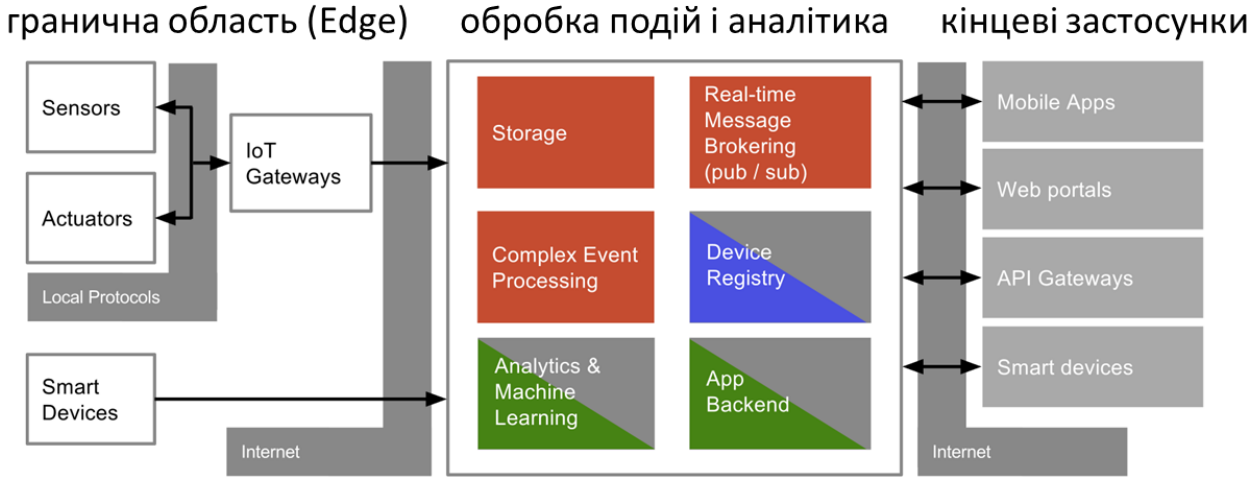

Рисунок 3.6 — Архітектура Інтернету речей

У рамках архітектури IoT за рекомендацією ITU Y.2060 взаємодія з фізичними об’єктами («речами») здійснюється через датчики (Sensors) та виконавчі механізми (Actuators). Вони розташовані на граничному (Edge) рівні, який забезпечує первинний збір даних і підключення до локальних мереж (Wi-Fi, Zigbee), глобальних (5G, супутникові) або ad-hoc.

Зібрані дані передаються на рівень обробки подій і аналітики (Platform/Event Processing) через Інтернет. Тут інформація:

- зберігається (Storage);
- обробляється в режимі реального часу (Stream Processing, Real-Time Message Brokering);
- направляється в потрібні сервіси та додатки;

- використовується для аналітики (Analytics) та машинного навчання (Machine Learning).

Також цей рівень відповідає за управління пристроями (Edge Device Management) та реєстрацію обладнання (Device Registry). Зазвичай він реалізується на основі хмарних (Cloud) або туманних (Fog) обчислень і відповідає за логіку, аналогічну до рівня SCADA та контролерів в АСУТП (без HMI).

Доступ до результатів аналізу, моніторинг стану та віддалене управління здійснюються через кінцеві додатки (Cloud Apps), які виступають у ролі інтерфейсу користувача (HMI) у класичних автоматизованих системах [52].

Системи управління пропускною здатністю і якістю обслуговування (QoS) в IoT мають унікальні риси порівняно з традиційними мережами. Важливо класифікувати трафік за пріоритетністю: наприклад, медичні дані повинні мати найвищий пріоритет, тоді як інформація від датчиків навколишнього середовища може передаватися з більш низьким.

Забезпечення високої доступності IoT-систем потребує балансу між надійністю та економічністю. Підтримка стандарту «п’яти дев’яток» (99,999% часу безперебійної роботи) може коштувати значно дорожче за основну систему, що стимулює розробку нових підходів щодо оцінки ризиків і оптимізації витрат.

Технічні обмеження IoT-пристроїв викликають унікальні проблеми у сфері безпеки та надійності. Неможливість впровадження традиційних захисних засобів на пристроях із малими ресурсами вимагає нових рішень, зосереджених на мережевій інфраструктурі та хмарних сервісах.

Масштабованість рішень стає критично важливою через швидке зростання кількості IoT-пристроїв. Застарілі моделі моніторингу та управління можуть виявитися неефективними при управлінні мільйонами пристроїв, що генерують величезні обсяги даних.

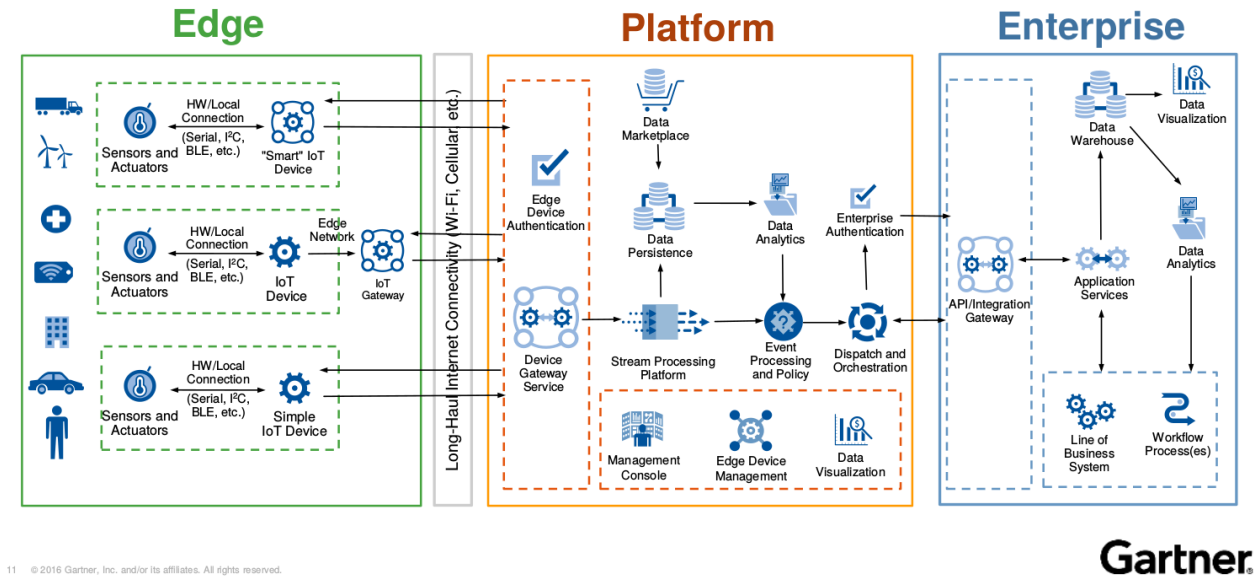

Рисунок 3.7 Розподілена обробка даних в IoT: локальні, хмарні та корпоративні рівні

Схема на рис.3.7 демонструє багаторівневу IoT-архітектуру, що складається з трьох основних шарів:

Edge (Периферійний рівень)

- Включає IoT-пристрої: датчики, актуатори, шлюзи.
- Виконує обробку даних локально, що знижує затримки та зменшує навантаження на мережу.
- Використовує локальні протоколи, такі як BLE, Zigbee, Serial.
- Особливо важливий для систем із вимогами реального часу, наприклад, у промисловому IoT.

Platform (Платформний рівень)

- Забезпечує зв’язок із хмарними сервісами через Wi-Fi, стільникові мережі тощо.
- Відповідає за агрегацію, зберігання та аналітику зібраних даних.
- Містить інструменти для машинного навчання (ML), потокової обробки подій (Event Processing) та API для інтеграції.

Enterprise (Корпоративний рівень)

- Включає бізнес-додатки (ERP, CRM) і системи візуалізації.
- Використовує дані для прийняття стратегічних рішень і автоматизації бізнес-процесів.

Архітектурні особливості та основні ризики:

- Слабка автентифікація користувачів і пристроїв.
- Проблеми з оновленням програмного забезпечення.
- Використання незахищених протоколів передачі даних.
- Обмежені ресурси IoT-пристроїв (пам’ять, енергоспоживання, обчислювальні можливості), що підвищує ризик кібератак.
- Висока залежність IoT-систем від мережевого середовища і нестабільність каналів зв’язку, що може спричинити каскадні збої.

Для досягнення високого рівня доступності необхідний комплексний підхід, який поєднує технічні рішення, стратегічне планування і постійний моніторинг систем.

3.2.2. Аналіз технологій обробки даних для підвищення ефективності мереж IoT.

Економічна та технічна ефективність IoT-системи значною мірою залежить від правильного вибору архітектури для обробки, зберігання та аналізу даних. Основні варіанти розміщення обчислювальних ресурсів включають:

- *Edge computing* — обробка даних безпосередньо на пристрої.
- *Fog computing* — обробка на рівні шлюзу або локальної мережі.
- *Cloud computing* — централізована обробка в хмарі.

Вибір між цими технологіями визначається потребами у затримці, пропускній здатності, масштабованості та обсягах обробки даних.

Нижче в Таблиці 3.1 наведено порівняння основних характеристик цих архітектур.

Таблиця 3.1 - Порівняння технологій обробки даних для IoT

Критерії	Edge computing	Fog computing	Cloud computing
Пропускна здатність	Низька (дані обробляються локально, зменшуючи трафік)	Середня (дані між пристроями, Fog-вузлами і хмарою)	Висока (залежить від обсягу, великий обсяг передач)
Затримка	Дуже низька (мілісекунди, обробка на пристрої)	Низька (десятки мілісекунд, обробка ближче до пристрою)	Висока (сотні мілісекунд, обробка далеко від пристрою)
Масштабованість	Низька (залежить від апаратного забезпечення)	Середня (можливе додавання Fog-вузлів)	Віртуально необмежена
Обробка даних	Локальна, в реальному часі	Локальна (на маршрутизаторах), більший обсяг обробки	У датацентрах із аналітикою BigData
Мережева залежність	Низька (робота автономно)	Середня (краще управляє непостійним підключенням)	Висока (залежність від стабільного інтернет-з'єднання)
Безпека	Середня (локальна обробка знижує ризик витоку, але вразливість до фізичних атак)	Середня (Fog-надає додатковий захист, потребує інтеграції)	Залежить від шифрування, ризик витоку під час передачі
Складність впровадження	Висока (налаштування пристроїв та ПЗ)	Середня (інтеграція Fog-вузлів із пристроями та хмарою)	Низька (хмарні платформи спрощують розгортання)

Щоб здійснити правильний вибір технологій обробки даних у IoT-системах, важливо враховувати типи даних, які генерують пристрої. Дані можуть варіюватися від простих числових значень до великих мультимедійних потоків, і їх класифікація допомагає визначити оптимальний спосіб обробки — локально на пристрої (Edge), на шлюзі (Fog) або в хмарі (Cloud) [56-57].

Класифікація типів даних IoT-пристроїв:

- Дані сенсорів: Температура, вологість, тиск — невеликі структуровані набори, до 1 МБ на день.
- Дані подій: Сповіщення про тривоги або нестандартні умови.
- Дані прискорення та геопозиції: Потоки від акселерометрів, гіроскопів, GPS — наприклад, GPS-трекер генерує близько 60 МБ на місяць.[58]

- Мультимедіа: Зображення або відео з IoT-камер, що генерують великі обсяги даних (6-10 ГБ на день для 1080p, 50-100 ГБ — для 4K) [59].
- Журнали роботи (логи): Статистика або діагностика, що передаються з певною періодичністю.
- Керуючі команди: Оновлення ПЗ, сигнали управління від хмари до пристроїв.
- Критично часочутливі дані: Для систем контролю польотів, охорони здоров'я, автономних транспортних засобів — вимагають обробки в реальному часі, наприклад, автівки генерують 1 ГБ інформації на секунду, Boeing 787 — до 5 ГБ на секунду[60].

Вибір архітектури обробки даних залежить від:

- Вимог до затримки: якщо потрібна обробка в реальному часі з мінімальними затримками — пріоритет за Edge/Fog.
- Обсягу даних: великі потокові дані (відео, аналітика) спочатку обробляють на Fog-узлах, потім передають у хмару; невеликі обсяги можна надсилати безпосередньо в хмару.
- Пропускної здатності: при обмеженнях її варто зменшувати фільтрацією на Edge/Fog для зниження трафіку.

Отже, оптимальне рішення — комбінований підхід: критично важливі та об'ємні дані обробляються безпосередньо на пристроях або в мережі (Edge/Fog), а вибіркові або підсумкові дані передаються до хмари для глибокого аналізу та зберігання.

3.2.3. Аналіз критеріїв оцінки підвищення ефективності мереж IoT

Оцінка ефективності використання мереж IoT можна розглянути на прикладі концепції «розумних міст» — однієї з найважливіших сфер застосування Інтернету речей, що має безпосередній вплив на життя громадян.

Сучасні «розумні» міста застосовують дані, технології та цифрову інфраструктуру для покращення транспортної системи, енергоефективності, управління відходами, моніторингу навколишнього середовища та безпеки

громадян. Зібрані дані допомагають адміністраціям оптимізувати ресурси, скоротити витрати та підвищити якість міських послуг.

Аналіз ефективності впровадження IoT у розумних містах важливий для обґрунтування інвестицій і поліпшення якості життя. Ефективність тут розуміється як досягнення поставлених цілей із мінімальними ресурсами та максимальним позитивним впливом, включаючи економічні, соціальні та екологічні аспекти.

Для оцінки використовують ключові показники (KPI) згідно з документом ITU-T Y.4903 (03/2022) «Key performance indicators for smart sustainable cities to assess the achievement of sustainable development goals»[21], розробленого Міжнародним союзом електрозв'язку (ITU).

– Категорія: *ІКТ інфраструктура*

Одним із важливих показників у категорії «ІКТ інфраструктура» є «*Покриття бездротового широкосмугового доступу*». Він вимірює частку території міста (км²), яка покрита мобільним інтернетом (3G, 4G, 5G) відносно загальної площі міста.

В Україні мобільне покриття ширше за фіксований інтернет, й у всіх великих містах вже присутній 4G-зв'язок[63], що є ключовою умовою для впровадження IoT-застосунків у розумних містах.

Отже, цей показник відображає ступінь готовності міської інфраструктури до ефективного використання технологій Інтернету речей.

$$STP_{моб} = \frac{Площа\ міста, вкрита\ мобільним\ Інтернетом(км^2)}{Загальна\ площа\ міста(км^2)} \times 100\ \% \qquad (3.1.)$$

– Категорія: *водопостачання та санітарія*

Показник «*ІКТ-моніторинг водопостачання*» оцінює ефективність використання систем моніторингу водопостачання, які застосовують інформаційно-комунікаційні технології для збору, аналізу та візуалізації даних про стан мережі водопостачання.

Визначається як відсоток довжини системи диспетчерського контролю та збору даних (SCADA), що контролюється за допомогою ІКТ (км), відносно загальної довжини мережі водопостачання (км). Цей показник відображає ступінь цифровізації управління водними ресурсами в місті.

$$STP_{вод} = \frac{Довжина\ системи\ диспетчерського\ контролю(км)}{Загальна\ довжина\ системи\ водопостачання(км)} \times 100 \ \% \qquad (3.2.)$$

Використання зазначених показників дає змогу розумним містам ефективно контролювати та оптимізувати водопостачання, що є важливим кроком для досягнення цілей сталого розвитку в цій сфері. Це дозволяє підвищити якість послуг, знизити втрати води та забезпечити надійність водопостачання для населення.

– Категорія: *електропостачання*

Показник «ІКТ-моніторинг електропостачання» визначає рівень впровадження систем SCADA у мережах IoT для централізованого збору, аналізу та обробки даних про електропостачання в режимі реального часу.

Застосування таких систем підвищує надійність електромереж, зменшує тривалість відключень і забезпечує економічно ефективну експлуатацію мережі.

Показник розраховується як відсоток довжини мережі диспетчерського контролю та збору даних (SCADA) електропостачання, яка управляється за допомогою ІКТ (км), відносно загальної довжини системи електропостачання (км).

$$STP_{електр} = \frac{Довжина\ системи\ диспетчерського\ контролю(км)}{Загальна\ довжина\ системи\ електростачання(км)} \times 100 \ \% \qquad (3.3.)$$

– Категорія: *транспорт*

«Динамічна інформація про громадський транспорт» визначає можливість міста надавати пасажирам актуальні дані про стан і рух громадського транспорту в режимі реального часу. Затори на дорогах — одна з головних проблем у сучасних містах, і розвиток громадського транспорту є

ефективним способом поліпшення мобільності населення. Завдяки використанню IoT-пристроїв, GPS-трекінгу та хмарних технологій можна не лише покращити користувацький досвід, але й допомогти операторам коригувати розклади, оптимізувати маршрути та ефективніше управляти ресурсами.

Показник розраховується як відсоток зупинок і станцій із доступною динамічною інформацією від загальної кількості зупинок і станцій у місті.

$$STP_{транс} = \frac{Кількість\ станцій\ з\ доступною\ інформацією}{Загальна\ кількість\ станцій} \times 100\ \% \qquad (3.4.)$$

«*Моніторинг дорожнього руху*» визначає здатність системи в режимі реального часу збирати і аналізувати інформацію про рух транспортних засобів на основних вулицях міста. Цей показник включає вимірювання швидкості руху, інтенсивності трафіку, виявлення заторів та аварійних ситуацій. Завдяки інтеграції IoT-пристроїв, відеокамер, GPS-трекінгу та хмарних технологій система може оперативно регулювати світлофори, перенаправляти транспортні потоки та інформувати громадян про ситуацію на дорогах. Це сприяє зменшенню заторів, скороченню часу в дорозі та підвищенню безпеки мешканців.[65]

Показник розраховується як відсоток довжини основних вулиць під контролем ІКТ (км) від загальної протяжності цих вулиць (км).

$$STP_{дорог} = \frac{Довжина\ вулиць,\ які\ контролюються\ ІКТ(км)}{Загальна\ протяжність\ основних\ вулиць} \times 100\ \% \qquad (3.5.)$$

– Категорія: *державний сектор*

«*Електронне урядування*» (e-government) оцінює рівень впровадження електронних державних послуг у розумних містах, що забезпечують зручний і швидкий доступ громадян до адміністративних послуг. Індикатор зосереджується на кількості доступних послуг, які можуть бути представлені через веб-сайти, мобільні додатки або текстові повідомлення. Завдяки інтеграції IoT-пристроїв і хмарних технологій, дані від громадян та державних

систем (наприклад, заявки на послуги, моніторинг інфраструктури) передаються до хмарних платформ для оперативної обробки й аналізу даних у реальному часі. Це сприяє підвищенню ефективності державного управління та покращенню доступу до послуг.

Показник розраховується як кількість публічних послуг, доступних громадянам через онлайн-сервіси.

$$STP_{послуг} = \frac{Кількість\ публічних\ послуг, доступних\ он-лайн}{Загальна\ кількість\ потрібних\ публічних\ послуг} \times 100 \quad \% \qquad (3.6.)$$

Загалом, впровадження мережевих технологій IoT є критично важливим етапом у розвитку розумних міст. Воно забезпечує централізоване управління, зберігання та обчислення даних, підвищує надійність і ефективність міських послуг, а також створює основу для впровадження інновацій. Аналіз ключових показників ефективності підтверджує потенціал IoT-систем у значному покращенні управління енергоспоживанням та водопостачанням, оптимізації транспортних потоків і якості комунальних послуг. Це сприяє формуванню нової парадигми міського середовища, орієнтованої на потреби жителів, що створює комфортніші, безпечніші та сталий розвиток міст.

3.2.4. Порівняльна характеристика методів підвищення ефективності мереж IoT з урахуванням вимог безпеки

Використання пристроїв Інтернету речей має багато переваг, таких як автоматизація, оптимізація процесів та створення нових сервісів, але водночас підвищує ризики, пов’язані з безпекою та конфіденційністю. Основні проблеми безпеки в IoT проявляються на трьох рівнях: пристроїв, мережі та даних.

На **рівні IoT-пристроїв** головною проблемою є обмежені обчислювальні ресурси, що ускладнює впровадження надійних методів шифрування даних. Зокрема:

– Обмеженість обчислювальної потужності ускладнює застосування сучасних алгоритмів шифрування, що підвищує ризик перехоплення або модифікації даних при передачі між пристроями, шлюзами чи хмарою.

– Слабкі методи аутентифікації та авторизації в багатьох IoT-пристроях спрощують зловмисникам отримання несанкціонованого доступу до системи.

На **рівні мережі** виникають такі проблеми безпеки:

– Використання незахищених мережевих інтерфейсів (Wi-Fi, Bluetooth, стільниковий зв’язок) створює легкі точки доступу для зловмисників, оскільки багато IoT-пристроїв підключені до Інтернету саме через ці канали.

– Якщо всі IoT-пристрої розміщені в одній мережі без розподілу на ізольовані сегменти, зловмисник, який отримає контроль над одним пристроєм, може легко переміщатися мережею і отримувати доступ до інших пристроїв та важливих частин системи.

– IoT-пристрої можуть швидко заражатися шкідливим ПЗ і перетворюватися на «зомбі» для створення ботнетів, які організовують масштабні DDoS-атаки та порушують роботу критично важливих сервісів.

На **рівні даних** існують такі проблеми безпеки та конфіденційності:

– Відсутність ефективних методів анонімізації під час аналізу чи обробки інформації може призвести до розкриття особистих даних користувачів. Це особливо гостро, враховуючи, що IoT-пристрої часто збирають чутливу інформацію, наприклад, про стан здоров’я, геопозицію та інші приватні дані.

– Нечітка політика доступу та відсутність визначених прав користувачів можуть створити ситуації, коли одні користувачі отримують доступ до даних інших без їхньої згоди.

– Через те, що IoT-пристрої є частиною взаємопов’язаної мережі, дані, зібрані одним пристроєм, можуть передаватися між різними платформами. При неналежному захисті це створює ризик витоку інформації третім особам, включно з виробниками, рекламодавцями або іншими користувачами.

3.2.5. Порівняльний аналіз протоколів за параметрами продуктивності, енергоефективності та безпеки

Ключові характеристики найбільш розповсюджених протоколів верхнього рівня IoT підсумовує Таблиця 3.2, що допомагає вибрати оптимальний варіант в залежності від конкретних вимог та обмежень системи.

Таблиця 3.2. Порівняльний аналіз протоколів рівня застосунків [63-65]

Протокол	Модель	Транспортний протокол	Експлуатаційні витрати	Енергоефективність	Типові механізми безпеки
MQTT	Publish/ subscribe	TCP	Низькі для малих повідомлень	Висока на вузьких каналах	SSL, аутентифікація на рівні брокера
DDS	Publish/ subscribe	TCP/UDP	Вищі, складна реалізація	Здебільшого не для обмежених вузлів	SSL/DTLS
CoAP	Publish/ subscribe	UDP	Дуже низькі	Дуже висока для обмежених вузлів	DTLS
AMQP	Broker - based messaging	TCP	Вищі через складні структури	Орієнтація на потужні пристрої	TLS, SASL
HTTP(S)	Запит - відповідь	TCP	Високі через заголовки	Нижча на обмежених вузлах	SSL/HTTPS

Висновки до розділу 3

У третьому розділі проведено ґрунтовний аналіз застосування мережевих технологій Інтернету речей, а також розглянуто економічну й технічну ефективність вибору технологій обробки даних залежно від типу трафіку, обсягів інформації, затримок і масштабованості системи. Особлива увага приділена трьом основним технологіям: Edge computing, Fog computing та Cloud computing, з визначенням їхніх сильних сторін і областей застосування.

Визначено, що Edge computing оптимальна для обробки даних у реальному часі, Fog computing балансує між швидкістю та ефективністю для обробки великих обсягів даних на рівні мережі, а Cloud computing забезпечує потужні можливості для аналітики та зберігання, хоча при великих обсягах даних його експлуатаційні витрати можуть бути суттєвими. З огляду на це рекомендовано використовувати комбінований підхід для ефективної роботи IoT-систем.

Розглянуто конкретні приклади застосування IoT: у розумних містах — для покращення міської інфраструктури, у промисловості (IIoT) — для підвищення ефективності виробництва, в охороні здоров'я — для дистанційного моніторингу пацієнтів.

Аналіз ефективності розумних міст на основі ITU-T Y.4903 демонструє великий потенціал мережевих IoT-технологій у таких сферах, як покриття бездротових мереж, моніторинг енергопостачання та водопостачання, транспортні системи, безпека дорожнього руху.

Сформульовано ключові методи підвищення ефективності мереж IoT:

- Збільшення продуктивності каналів передачі інформації, зокрема з використанням сучасних оптоволоконних технологій, що дозволяє обслуговувати більше IoT-об'єктів і пришвидшити їх реакцію.
- Вдосконалення технологій бездротового доступу, таких як 5G, 6G та специфічні IoT-протоколи, що також підвищує кількість підключених об'єктів і швидкість взаємодії.
- Активне використання хмарних технологій для оптимальної обробки та зберігання даних IoT, що пришвидшує реакцію систем і раціоналізує використання мережевих ресурсів.
- Використання сучасних технологій кіберзахисту для захисту IoT-мереж від зовнішніх загроз і несанкціонованого доступу.

Ці заходи формують фундамент для створення надійних, ефективних і безпечних IoT-мереж, які сприятимуть розвитку інноваційного та сталого середовища сучасного міста.

ВИСНОВКИ

Дипломна робота присвячена дослідженню застосування мережних технологій в Інтернеті речей (IoT), що є важливою темою сучасної цифрової трансформації. Для цього було вивчено широкий набір джерел: навчальні посібники, наукові публікації, стандарти ITU-T та NIST, рекомендації IEEE, а також аналітичні звіти та статті від провідних фахівців. Це дозволило надати всебічну оцінку як технічних, так і економічних аспектів.

Перший розділ присвячений детальному розгляду технологій IoT.

Визначена роль мережних технологій як ключового інструменту для підтримки систем IoT, що забезпечують обробку, зберігання та аналіз даних у реальному часі. Показано різні сфери застосування IoT — від розумного будинку до медицини, промисловості, розумних міст і автономного транспорту. Розглянуто моделі хмарних обчислень і 7-рівневу архітектуру IoT-систем. Описані переваги і виклики як окремо цих технологій, так і їх інтеграції в масштабні IoT-системи.

Також проаналізовано ряд проблем, які залишаються викликами:

- Захист безпеки і конфіденційності даних.
- Мережеві затримки.
- Залежність від стабільного інтернет-з’єднання, що ускладнює впровадження хмарних технологій і IoT.

У другому розділі дослідження розглядаються перспективи розвитку мережних технологій в Інтернеті речей (IoT). Тут проведено аналіз ключових тенденцій і інновацій, які зумовлюють стрімке зростання світового ринку IoT. Зокрема, розглядаються технології проводових і безпроводових мереж, таких як 5G, Wi-Fi 6, LPWAN, а також хмарні та безпекові рішення.

Особливу увагу приділено проблемам інтеграції мережних технологій з іншими компонентами IoT. Запропоновано методи їх вирішення, зокрема:

- використання просунутих алгоритмів шифрування даних,
- створення ізольованих мережевих сегментів,
- впровадження багаторівневої аутентифікації.

У третьому розділі проведено детальний аналіз прикладів застосування мережних технологій у IoT:

- розглянуто обробку даних від IoT-пристроїв,
- порівняно граничні (edge), туманні (fog) та хмарні обчислювальні технології,
- запропоновано методику вибору технологій для ефективної обробки IoT-трафіку, що дозволяє збалансувати високу продуктивність, економію ресурсів і забезпечити централізоване та віддалене керування.

Також визначено критерії оцінки методів підвищення ефективності мереж IoT, які підкреслюють важливість комбінування різних технологій при створенні IoT-систем.

Робота містить аналіз застосування мережних IoT-технологій на реальних прикладах:

- у «розумних» містах, де мережі забезпечують ефективне управління інфраструктурою та покращення міських послуг,
- у промисловості для оптимізації виробничих процесів,
- у сфері охорони здоров’я для дистанційного моніторингу пацієнтів.

Крім того, проведено комплексний аналіз ефективності мережевих IoT-систем у розумних містах на основі документа ITU-T Y.4903, включаючи сфери ІКТ, водопостачання, електропостачання, транспорт і державний сектор. Результати підтвердили високу ефективність впровадження IoT для досягнення цілей сталого розвитку.

Основні методи підвищення ефективності мереж Інтернету речей (IoT) сформульовано, обґрунтовано та ілюстровано таким чином:

- Збільшення продуктивності каналів передачі інформації в мережевій інфраструктурі за допомогою сучасних і перспективних технологій, зокрема оптоволоконних. Показником ефективності є зростання кількості IoT-об’єктів у специфічній інфраструктурі та прискорення їх реакції.
- Вдосконалення технологій безпроводового доступу до IoT-пристроїв у загальній інформаційній мережі (технології 5G, 6G) та у специфічній IoT-інфраструктурі відповідно до діючих безпроводових стандартів. Вимір

ефективності — подібне збільшення кількості об’єктів і швидкості їх взаємодії.

- Використання хмарних технологій для операцій із IoT-об’єктами, що забезпечує швидшу реакцію пристроїв та більш раціональне використання мережевих ресурсів.
- Застосування кіберзахисту мереж IoT, спрямованого на захист IoT-об’єктів від зовнішніх небажаних втручань. Ефективність визначається рівнем безпеки в специфічній IoT-інфраструктурі.

Ці методи дозволяють підвищити масштабованість, продуктивність, безпеку та надійність мереж Інтернету речей.

Майбутнє Інтернету речей (IoT) виглядає багатообіцяючим з численними інноваціями для бізнесу:

- **Зростання** кількості пристроїв: Очікується, що їх число протягом наступних років досягне десятків мільярдів через ширше впровадження IoT у різних галузях і розвиток нових сценаріїв використання.
- **Периферійні обчислення**: Вони набирають вагу, оскільки дозволяють обробляти та аналізувати дані ближче до джерела, що знижує затримки, покращує час відгуку і зменшує навантаження на мережі.
- **Штучний інтелект і машинне навчання**: Ці технології допомагають аналізувати великі обсяги даних з IoT-пристроїв, що сприяє прийняттю обґрунтованих рішень і оптимізації діяльності підприємств.
- **Блокчейн**: Досліджується для покращення безпеки і конфіденційності IoT, дозволяючи будувати децентралізовані стійкі мережі та знижувати ризики втручання.
- **Сталий розвиток**: IoT сприяє ефективнішому використанню ресурсів, енергії та зменшенню відходів у різних галузях, що важливо для екологічної сталості.

Зниження вартості виробництва IoT-пристроїв і зростання їх кількості стимулює компанії до адаптації і використання нових технологій та сценаріїв застосування з метою отримання конкурентних переваг.

У результаті виконання роботи всі поставлені завдання були успішно реалізовані, а її мета досягнута. Здійснено дослідження та аналіз інтеграції технології Інтернету речей (IoT) з мережевими, особливо безпроводовими, у поєднанні з хмарними та безпековими технологіями. Проведено оцінку переваг і викликів такої інтеграції та визначено перспективи подальшого розвитку для розробки ключових методів підвищення ефективності IoT-мереж.

Розглянуто вплив інтегрованих технологій на управління даними, безпеку, інноваційний розвиток, а також взаємодію між хмарними технологіями та Інтернетом речей. Отримано ґрунтовні знання у сфері перспективних IoT-мереж, які можуть бути використані для подальшого розвитку і реалізації хмарних IoT-рішень у різних галузях.

Дослідження підтвердило важливість застосування мережних технологій в Інтернеті речей і довело їх перспективність та ефективність у поєднанні з хмарними і безпековими технологіями.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ЗАКОН УКРАЇНИ Про Національну програму інформатизації. https://zakon.rada.gov.ua/laws/show/2807-20#Text

2. ЗАКОН УКРАЇНИ Про електронні комунікації. https://zakon.rada.gov.ua/laws/show/1089-20#Text

3. НАКАЗ Про затвердження критеріїв для віднесення електронних комунікаційних мереж до мереж широкосмугового доступу, високошвидкісних мереж, мереж високої та надвисокої пропускної здатності. https://zakon.rada.gov.ua/laws/main/z1786-24?utm_source=chatgpt.com#Text

4. ЗАКОН УКРАЇНИ Про захист інформації в інформаційно-комунікаційних системах: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

5. Заїка В.Ф., Варфоломеєва О.Г., Домрачева К.О., Гринкевич Г.О. Телекомунікаційні системи та мережі наступного покоління. – Київ – 2019. - 315 с. – ДУІКТ

6. What is the IoT? [електронний ресурс] // IBM. URL: https://www.ibm.com/topics/internet-of-things

7. Satyajit Sinha. State of IoT 2024. – [електронний ресурс] URL: https://iot-analytics.com/number-connected-iot-devices/

8. Mohit Angurala, Prabh Deep Singh. Integration of Cloud Computing and IoT. 2024 – [електронний ресурс] URL: https://drive.google.com/file/d/1WNoRWlMKyvLjpricYmjZHI3L7QM0H8zF/view

9. Thomas Erl, Eric Barcelo. Cloud Computing Concepts, Technology, Security, and Architecture. – [електронний ресурс] 2023. URL: https://drive.google.com/file/d/1IVuN1TXe2Z8NTrxkz95Nu-z4vrxUjv3j/view

10.Що таке інтернет речей або IoT? [Електронний ресурс] URL:https://edin.ua/shho-take-internet-rechej-abo-iot/

11. Zerkliny V. Інтернет речей: поняття, архітектура та протоколи. Журнал «Телекомунікації», № 1, 2022 – ДУІКТ.

12. Yadav, P., Li, Q., & Mortier, R. (2018). IoT network behaviors and dependencies (Series No. CDBB_WP_005). University of Cambridge.

https://www.cdbb.cam.ac.uk/system/files/documents/2018CDBB_WP_005_IOTNetworkBehaviours.pdf

13. Mike Thomas, Matthew Urwin. 30 Internet of Things Examples You Should Know. 2024 – [електронний ресурс] URL: https://www.itransition.com/blog/iot-history

14. International Telecommunication Union. (06/2012). Overview of the Internet of things. ITU-T Recommendation Y.4000/Y.2060. – [електронний ресурс] URL: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=11559

15. [Електронний ресурс] URL: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=11559

16. An overview of IoT architectures, technologies, and existing open-source projects. 2022 – [електронний ресурс] URL: https://www.sciencedirect.com/science/article/pii/S254266052200107X?via%3Dihub#sec1

17. [Електронний ресурс] URL: https://www.sciencedirect.com/science/article/pii/S254266052200107X?via%3Dihub#sec1)

18. What Are the 7 Layers of IoT Architecture? [Електронний ресурс] URL: https://jelvix.com/blog/iot-architecture-layers

19. Original Article: by Domínguez Pérez Dannika Yelizavet , Orocio Méndez Florentino «Internet of Things Platform (IoT) - Comparison of Layered Architectures» URL: https://www.ijcttjournal.org/Volume-67%20Issue-1/IJCTT-V67I1P102.pdf

20. Architecture of Internet of Things (IoT) [Електронний ресурс] URL: https://www.geeksforgeeks.org/computer-networks/architecture-of-internet-of-things-iot/

21. Рекомендація MCE-T Y.2069 https://www.itu.int/rec/T-REC-Y.4903-202203-I/en/

22. За завісами магії IoT: пояснення архітектури IoT [Електронний ресурс] // Блог компанії PNN. URL: https://pnn.com.ua/ua/blog/detail/behind-the-curtains-of-iot-magic-iot-architecture-explained

23.Організація комп'ютерних мереж: https://ela.kpi.ua/server/api/core/bitstreams/e0a0c843-a57d-4d82-8f42-0eba294bef1f/content

24. Комп'ютерні мережі:

https://eir.zp.edu.ua/server/api/core/bitstreams/2e43f256-9a4e-4555-bf19-f83daf8dc3bd/content

25. Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing. – [електронний ресурс] URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

26. Stephanie Susnjara, Ian Smalley. What is cloud computing? [електронний ресурс] // IBM. URL: https://www.ibm.com/topics/cloud-computing

27. Khan, H. U., Ali, F., Alshehri, Y., & Nazir, S. Towards Enhancing the Capability of IoT Applications by Utilizing Cloud Computing Concept. 2022 [електронний ресурс] URL: https://doi.org/10.1155/2022/2335313

28. Mohit Angurala, Prabh Deep Singh. Integration of Cloud Computing and IoT. 2024 – [електронний ресурс] URL: https://drive.google.com/file/d/1WNoRWlMKyvLjpricYmjZHI3L7QM0H8zF/view

29. Heorhii Kuchuk, Eduard Malokhvii. Integration of IoT with Cloud, Fog, and Edge Computing: A Review. [електронний ресурс] URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/98c2c750-1de1-49cc-a749-79216f65e61a/content

30. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey [Електронний ресурс] URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC6165453/#sec5-sensors-18-02796

31. Комп'ютерні мережі. Посібник 1. Б.Ю. Жураковський, І.О. Зенів: content

32. Широкосмуговий інтернет: Широкосмуговий інтернет: що це таке та як працює? - LinkCom; МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ Методичні вказівки для виконання курсового проекту«ПРОЕКТУВАННЯ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ»: (MicrosoftWord - \302\321\305.doc)

33.Організація комп'ютерних мереж: [Електронний ресурс] URL: https://ela.kpi.ua/server/api/core/bitstreams/e0a0c843-a57d-4d82-8f42-0eba294bef1f/content

34. Комп'ютерні мережі / Електронний посібник. URL: https://km.ptngu.com/lections/2.html#:~:text=%D0%A2%D0%BE%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F%20%D0%BA%D0%BE%D0%BC%D0%BF'

%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D1%97%20%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96%20%E2%80%93%20%D1%86%D0%B5,%D0%BD%D0%B0%D0%B4%D1%96%D0%B9%D0%BD%D1%96%D1%81%D1%82%D1%8C%20%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D0%B8%2C%20%D0%BC%D0%BE%D0%B6%D0%BB%D0%B8%D0%B2%D0%BE%D1%81%D1%82%D1%96%20%D1%80%D0%BE%D0%B7%D1%88%D0%B8%D1%80%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96

35. Wireless IoT Network. [Електронний ресурс] URL: https://www.siemens.com/uk-ua/products/wittra-networks-ab-wireless-iot-network/

36. [Електронний ресурс] URL: Wi-Fi/802.11: https://www.wi-fi.org

37.Zigbee застосування: [Електронний ресурс] URL: https://zigbeealliance.org

38. Перелік протоколів, технологій на кожному рівні мережевої моделі: [Електронний ресурс] URL: https://azure.microsoft.com/ru-ru/solutions/iot/iot-technology-protocols

39. Мережі LPWAN: [Електронний ресурс] URL: https://www.gsma.com/iot/lpwa

40. What is Wi-Fi HaLow or 802.11ah. [Електронний ресурс] URL: https://www.eWi-Fi HaLow

41. [Електронний ресурс] URL:.https://volansys.medium.com/

42.Перелік протоколів, технологій на кожному рівні мережевої моделі: [Електронний ресурс] URL: https://azure.microsoft.com/ru-ru/solutions/iot/iot-technology-protocols

43. How much data does a security camera use per day? [електронний ресурс] URL: https://solink.com/resources/industry-insights/how-much-data-does-a-security-camera-use-per-day/

44.Мережева модель OSI: [Електронний ресурс] URL: https://kr-labs.com.ua/blog/model-osi

45.Стек протоколів TSP/IP: [Електронний ресурс] URL: https://vlplk.blogspot.com/2017/12/osi.html

46.Стек протоколів TSP/IP: [Електронний ресурс] URL: https://www.guru99.com/uk/tcp-ip-model.html

47.Порівняння мережевої моделі OSIта стеку протоколів TSP/IP: [Електронний ресурс] URL: https://vlplk.blogspot.com/2017/12/osi.html

48. [Електронний ресурс] Промисловий стандарт tcp/ip. Переваги та недоліки моделей osi/iso і tcp/ip.

49.Міжмережевий рівень: [Електронний ресурс] URL: https://www.netacad.com, https://e-tk.lntu.edu.ua/mod/page/view.php?id=3547

50. InternetProtocol Specification: [Електронний ресурс] RFC 793 - Протокол управління передачею

51. Рівень доступу до мережі: [Електронний ресурс] Модель TCP/IP: що таке рівні та протокол? Стек TCP/IP

52. Школа автоматики. Технології індустрії 4.0: Лекція 1. Основи Інтернету Речей [Електронний ресурс]. URL: http://edu.asu.in.ua/mod/book/tool/print/index.php?id=112

53. Fog Computing vs Edge Computing: Which is the Better Approach? 2025 [електронний ресурс] URL: https://cyberpanel.net/blog/fog-computing-vs-edge-computing

54. Cloud Computing or Edge Computing: Cost Comparison [електронний ресурс] URL: https://www.azion.com/en/blog/cloud-computing-or-edge-computing-cost/

55. Difference between Cloud, Fog and Edge Computing in IoT. 2022 [електронний ресурс] URL: https://www.digiteum.com/cloud-fog-edge-computing-iot/

56. Data Types and Data Structures. 2024 [електронний ресурс] URL: https://www.bigdataframework.org/knowledge/data-types-and-data-structures/

57. Anna Gerber, Satwik Kansal. Making sense of IoT data [електронний ресурс] URL: https://developer.ibm.com/tutorials/iot-lp301-iot-manage-data/

58. Morgan Hightower. How Much Data Does a GPS Tracker Use. 2024 [електронний ресурс] URL: https://trackhawkgps.com/blog/how-much-data-does-a-gps-tracker-use#:~:text=Average%20Data%20Consumption,to%20over%2020%20MB%20monthly

59. How much data does a security camera use per day? [електронний ресурс] URL: https://solink.com/resources/industry-insights/how-much-data-does-a-security-camera-use-per-day/

60. Li Yang, Abdallah Shami. IoT Data Analytics in Dynamic Environments: From an Automated Machine Learning Perspective. 2022 [електронний ресурс] URL: https://arxiv.org/pdf/2209.08018

61.https://uk.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B1%D1%96%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9_%D0%B7%D0%B2%27%D1%8F%D0%B7%D0%BE%D0%BA_%D0%B2_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96

62. Performance Measures for Traffic Signal Systems: An Outcome-Oriented Approach. 2014 – [електронний ресурс] URL: https://www.researchgate.net/publication/263962649_Performance_Measures_for_Traffic_Signal_Systems_An_Outcome-Oriented_Approach#pf7f

63. IoT Protocols and Standards Worth Exploring in 2024 [Електронний ресурс] URL: https://www.emqx.com/en/blog/iot-protocols-mqtt-coap-lwm2m#5-mqtt

64. IoT Protocols: A comprehensive guide for enterprises [Електронний ресурс] URL: https://www.a1.digital/knowledge-hub/iot-protocols-a-comprehensive-guide/

65. Optimizing IoT Protocols for Edge Microservices [Електронний ресурс] URL: https://blog.dreamfactory.com/optimizing-iot-protocols-for-edge-microservices

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Методи підвищення ефективності мереж Інтернету речей

Дипломна робота на здобуття ступеня бакалавра

ВИКОНАВ:
Студент IV курсу, групи ІСД-41
Гудим Олександр Олександрович

КЕРІВНИК:
кандидат технічних наук
Олег Синьков

Актуальність та мета дослідження

Актуальність: Вибухове зростання кількості IoT-пристроїв (18.8+ млрд) вимагає радикальної оптимізації мережевих ресурсів для уникнення колапсу інфраструктури.

Мета: Розробка та обґрунтування методів підвищення продуктивності мереж через гібридну архітектуру обробки даних.

Об'єкт дослідження
Мережеві безпроводові технології у взаємодії з хмарними та безпековими сервісами в структурі IoT.

Концептуальна формула IoT

Ефективність системи Інтернету речей базується на синергії компонентів:

IoT = Сенсори + Дані + Мережі + Послуги

Збір	Аналіз	Транспорт	Цінність

Семирівнева архітектура IoT систем

Рівень 7	Application Layer: Бізнес-процеси та інтерфейси.
Рівень 6	Data Abstraction: Фільтрація та збереження у БД.
Рівень 5	Data Accumulation: Агрегація та черги повідомлень.
Рівень 4	Transport / Gateway: Маршрутизація пакетів.
Рівень 3	**Connectivity: Специфічна мережева інфраструктура (Фокус роботи).**
Рівень 2	Edge Computing: Первинна обробка на місцях.
Рівень 1	Physical Devices: Датчики та актуатори.

Критерії якості обслуговування (QoS)

Продуктивність
Здатність мережі обробляти пікові навантаження без втрат пакетів.

Латентність
Мінімальна затримка для критичних систем реального часу.

Енергоощадність
Максимізація терміну служби автономних вузлів IoT (до 10 років).

Порівняльний аналіз стандартів зв'язку

Стандарт	Радіус дії	Швидкість	Енергоспоживання
Wi-Fi HaLow	до 1 км	0.15 – 80 Мбіт/с	Низьке
BLE	до 100 м	до 2 Мбіт/с	Дуже низьке
Zigbee	до 100 м	250 Кбіт/с	Низьке
LoRaWAN	до 15 км	до 50 Кбіт/с	Мінімальне
NB-IoT	до 15 км	до 250 Кбіт/с	Мінімальне

Вибір технології визначається балансом між швидкістю та автономністю.

Методи обробки трафіку: Edge, Fog, Cloud

Edge Computing
Обробка на самому пристрої. Найменша затримка, висока конфіденційність.

Fog Computing
Обчислення на рівні шлюзів. Агрегація даних від групи локальних вузлів.

Cloud Computing
Централізована обробка. Глибока аналітика та тривале зберігання Big Data.

Застосування хмарних технологій в IoT

Хмарні сервіси дозволяють IoT-системам виходити за межі локальних обчислень, забезпечуючи:

- **IaaS:** Масштабовану інфраструктуру;
- **PaaS:** Платформи для швидкої розробки;
- **SaaS:** Готові аналітичні інструменти.

Зниження витрат на IT-інфраструктуру до 40%.

Аналіз Smart City (ITU-T Y.4903)

Критерії оцінки за міжнародним стандартом:

- **Transport:** Адаптивні світлофори, моніторинг заторів.
- **Utilities:** SCADA-моніторинг ресурсів.
- **E-Gov:** Електронні державні послуги.
- **Ecology:** Датчики якості повітря та шуму.

Ефективність: Оптимізація ресурсів міста сягає 30%.

Покращення впровадження «розумних» рішень

Сектор	Показник покращення в місті	Ефект (%)
Безпека	Запобігання летальним наслідкам (ДТП, пожежі)	8 – 10 %
	Запобігання злочинним нападам (крадіжки, напади)	30 – 40 %
	Зменшення часу реагування на надзвичайні ситуації	30 – 35 %
Час	Зменшення часу пересування містом	15 – 20 %
	Економія часу у взаємодії з урядом та охороною здоров'я	45 – 65 %
Здоров'я	Зниження рівня захворюваності	8 – 15 %
Довкілля	Запобігання викидам парникових газів (ПГ)	10 – 15 %
	Зменшення непорахованих відходів	10 – 20 %
Соціум	Зменшення рівня самотності / Зв'язок з громадою	20 – 30 %
	Частка жителів, які відчувають зв'язок з владою	20 – 30 %
Робота	Зростання офіційної зайнятості	1 – 3 %
Витрати	Зменшення щомісячних витрат (прожитковий мінімум)	1 – 2 %

Джерело: "Smart-інфраструктура у сталому розвитку міст: світовий досвід та перспективи України"

Порівняння прикладних протоколів

Протокол	Модель	Транспорт	Навантаження
MQTT	Pub / Sub	TCP	Дуже низьке (Найкраще для IoT)
CoAP	Req / Res	UDP	Мінімальне (Обмежені вузли)
AMQP	Broker	TCP	Середнє (Надійність)
HTTP/S	Req / Res	TCP	Високе (Неефективно)

MQTT є стандартом де-факто для IoT-рішень через малий заголовок.

Методи підвищення ефективності мереж

Гібридна обробка
Впровадження Edge/Fog обчислень для розвантаження магістралей.

Оптимізація трафіку
Використання MQTT/CoAP для мінімізації мережевих оверхедів.

Легка безпека
Впровадження енергоефективних алгоритмів шифрування.

Загальні висновки

- Доведено, що **ефективність мережі** залежить від балансу між локальною обробкою (Edge) та хмарою.
- Визначенно, що **NB-IoT** як оптимальний стандарт для масштабних енергоефективних мереж.
- Аналіз показників **ITU-T** підтвердив економічну вигоду впровадження IoT у Smart City (до 30%).
- Обґрунтовано вибір **MQTT** як основного протоколу для оптимізації передачі трафіку.

Дякую за увагу!

Готовий відповісти на Ваші запитання

Гудим Олександр Олександрович
Київ – 2026